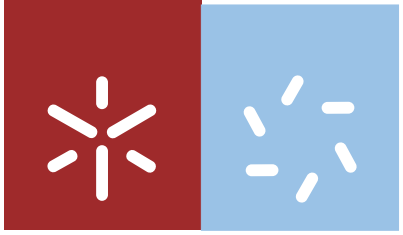
Universidade do Minho
Escola de Ciências

António José Ribeiro Caldas Domingues

Monóides Comutativos Finitamente Gerados

Maio de 2013

Monóides Comutativos Finitamente Gerados
António José Ribeiro Caldas Domingues
UMinho | 2013



Universidade do Minho
Escola de Ciências

António José Ribeiro Caldas Domingues

Monóides Comutativos Finitamente Gerados

Dissertação de Mestrado
Mestrado em Ciências – Formação Contínua de Professores
Área de Especialização em Matemática

Trabalho realizado sob a orientação da
Doutora Maria Paula Marques Smith

Maio de 2013

António José Ribeiro Caldas Domingues

Endereço eletrónico: domingues.toze@gmail.com

Título da dissertação: Monóides Comutativos Finitamente Gerados

Orientadora: Doutora Maria Paula Marques Smith

Ano de conclusão: 2013

Mestrado em Ciências- Formação Contínua de Professores, Ramo Matemática

Universidade do Minho, de 2013

O autor: António José Ribeiro Caldas Domingues

AGRADECIMENTOS

Agradeço a todas as pessoas que tornaram possível a realização deste trabalho. Gostaria de expressar a minha gratidão de modo particular:

À Doutora Maria Paula Marques Smith, orientadora deste trabalho, pelo apoio, paciência e total disponibilidade.

Às colegas e amigas, Florbela Ribeiro e Rosa Marinho, pelo apoio e incentivo.

À colega e amiga Helena Ferreira, pela ajuda preciosa com o ”Latex”.

Aos meus queridos pais, Justino Domingues e Aurora Ribeiro e à minha irmã, Cristina Domingues, pelo carinho e incentivo.

À minha querida madrinha, Maria Elisa Domingues, pelo carinho, amizade e incentivo constante.

À minha amiga e amiga da minha família, Emília Alves, por toda a ajuda.

Ao meu primo, Miguel Domingues, pela sua amizade.

Aos meu amigos Jorge Pereira e Rui Sousa, pelo incentivo.

RESUMO

Um *monóide* é um semigrupo com identidade e um *monóide cancelativo* é um monóide que satisfaz a lei do corte. O objetivo deste trabalho é estudar uma classe especial de monóides comutativos, cancelativos e finitamente gerados: a classe de tais monóides que são finitos.

Depois de apresentarmos conceitos básicos e resultados preliminares, provamos que todo o monóide comutativo finitamente gerado é isomorfo a um quociente de $\mathbb{N}^p$, $p \in \mathbb{N}$, por uma certa congruência em $\mathbb{N}^p$. Mostramos ainda que, se o monóide dado é também cancelativo então ele é isomorfo a um submonóide de um grupo comutativo finitamente gerado.

Assim, estudamos de seguida os grupos abelianos finitamente gerados e provamos o teorema de estrutura para esta classe de grupos. Com base neste teorema, provamos que todo o monóide comutativo, cancelativo e finitamente gerado é, a menos de isomorfismo, um submonóide de $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$, para certos $d_1, d_2, \ldots, d_r, k \in \mathbb{N} \setminus \{0\}$.

Por fim, estudamos os monóides comutativos e cancelativos que são finitos: estes monóides são, naturalmente, finitamente gerados e, portanto, as conclusões do estudo anterior podem ser-lhes aplicadas. Demonstramos que a classe dos monóides comutativos cancelativos finitos coincide com a classe dos grupos finitos

ABSTRACT

A *monoid* is a semigroup with identity and a *cancellative monoid* is a monoid that satisfies the cancellation law. The purpose of this thesis is to study a special class of finitely generated commutative monoids that are cancellative: the class of such monoids that are finite.

After presenting basic concepts and preliminary results, we prove that every finitely generated commutative monoid is isomorphic to a quocient of $\mathbb{N}^p$, $p \in \mathbb{N}$, by a certain congruence on $\mathbb{N}^p$. We also show that if, in addition, the monoid is cancellative, then it is isomorphic to a submonoid of a finitely generated commutative group.

The study of finitely generated commutative groups is, therefore, necessary for achieving our objectives. We prove the structure theorem for this class of groups. On the basis of this theorem we show that every finitely generated commutative monoid that is cancellative is, up to isomorphism, a submonoid of $\mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$, for certain $d_1, d_2, ..., d_r, k \in \mathbb{N} \setminus \{0\}$.

Finally, we study commutative and cancellative monoids that are finite: naturally, these monoids are finitely generated and so the conclusions of the previous study can be applied. We prove that the class of commutative, cancellative finite monoids coincide with the class of finite groups.

Índice

1 Definições, resultados preliminares e notações **3**

1.1 Conceitos e resultados básicos 3

1.2 Congruências 9

1.3 Morfismos 11

1.4 Monóides finitamente gerados 14

2 Grupos comutativos finitamente gerados **21**

2.1 Base e dimensão de um subgrupo de $\mathbb{Z}^n$ 21

2.2 Matrizes com entradas inteiras e fatores invariantes de um subgrupo de $\mathbb{Z}^n$ 27

3 Monóides cancelativos finitos **47**

Bibliografia **54**

Introdução

De acordo com J. C. Rosales e P. A. García-Sánchez, em teoria de semigrupos, o estudo de monóides comutativos, cancelativos e finitamente gerados é muito importante, em particular, pela larga gama de aplicações que estas estruturas têm em vários campos da Álgebra: geometria algébrica, álgebra comutativa, teoria de números, álgebra computacional.

O objetivo deste trabalho é estudar uma classe especial de monóides comutativos, cancelativos e finitamente gerados: a classe dos monóides que são finitos.

No capítulo 1, apresentamos conceitos básicos e resultados preliminares. O estudo das relações de equivalência, congruências e propriedades dos morfismos, são fundamentais para este trabalho. Ainda neste capítulo, provamos que todo o monóide comutativo finitamente gerado é isomorfo a um quociente de $\mathbb{N}^p$, $p \in \mathbb{N}$, por uma certa congruência. Mostramos ainda que, se o monóide dado for também cancelativo, ele é isomorfo a um submonóide de um grupo comutativo finitamente gerado.

O estudo de grupos comutativos finitamente gerados torna-se assim fundamental. O segundo capítulo deste trabalho é, por essa razão, dedicado ao estudo dos grupos comutativos finitamente gerados. Na primeira secção, consideramos o grupo aditivo $\mathbb{Z}^n$, $n \in \mathbb{N}$, e estudamos conceitos análogos aos estudados em espaços vetoriais sobre um corpo: combinação linear de elementos do grupo $\mathbb{Z}^n$, base de um subgrupo de $\mathbb{Z}^n$, dimensão de um subgrupo de $\mathbb{Z}^n$ e isomorfismo de subgrupos de $\mathbb{Z}^n$. Na segunda secção, são estudadas matrizes com entradas inteiras. O estudo destas matrizes é, em tudo, análogo ao estudo das matrizes com entradas num corpo K qualquer. O processo de eliminação de Gauss-Jordan numa matriz com entradas num corpo K permite transformar uma matriz qualquer numa matriz da forma $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ que é equivalente à matriz inicial. Mostramos que qualquer matriz com entradas inteiras é equivalente a uma matriz da forma $\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$, onde D é uma matriz diagonal. Os elementos dessa matriz diagonal são de-

signados por *fatores invariantes* de *D*. Como veremos, por $\mathbb{Z}$ não ser corpo, o procedimento de "transformação" da matriz inicial numa matriz da forma referida não é tão simples como no caso de matrizes com entradas num corpo.

Ainda nesta secção, apresentamos exemplos que ilustram algumas diferenças nos procedimentos com matrizes com entradas inteiras. Os resultados obtidos para estas matrizes são importantes na medida em que são "traduzidos" para subgrupos de $\mathbb{Z}^n$. Definimos *fatores invariantes de um subgrupo M* e "equações" de *M* relativamente à base canónica de $\mathbb{Z}^n$. Munidos com estes resultados, enunciamos e demonstramos o teorema de estrutura para grupos comutativos finitamente gerados: *qualquer grupo comutativo finitamente gerado é isomorfo a um produto direto de grupos* $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$*, para certos naturais* $d_1, d_2, \ldots, d_r, k \in \mathbb{N} \setminus \{0\}$.

No terceiro capítulo desta dissertação, estudamos os monóides cancelativos que são finitos. Monóides cancelativos finitos são, naturalmente, finitamente gerados. Com base no estudo feito nos capítulos anteriores, obtemos que qualquer monóide cancelativo finitamente gerado é isomorfo a submonóide de $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$. Começamos, assim, por considerar um monóide cancelativo finitamente gerado *S* e identificar o submonóide de $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$ isomorfo a *S*. Provamos de seguida que a classe dos monóides cancelativos finitos coincide com a classe dos grupos finitos e vemos como é que isso se reflete nas equações do subgrupo de $\mathbb{Z}^n$ associado ao monóide inicial.

Capítulo 1

Definições, resultados preliminares e notações

Este capítulo é constituído por quatro secções. Nas três primeiras secções relembramos definições e resultados básicos gerais. Na última secção, são introduzidas definições e apresentados resultados relativos a monóides comutativos finitamente gerados.

1.1 Conceitos e resultados básicos

Comecemos por recordar a noção de semigrupo.

Definição 1.1.1. *Um **semigrupo** é um par $(S,\cdot)$ em que S é um conjunto não vazio e $\cdot$ uma operação binária, definida em S, que satisfaz a propriedade associativa, ou seja, tal que:*

$$\forall a,b,c \in S\colon\ (a\cdot b)\cdot c = a\cdot(b\cdot c).$$

Como veremos na Secção 4 deste capítulo, todo o monóide finitamente gerado é isomorfo a um submonóide de um grupo aditivo. Por esta razão, usaremos, nesta monografia, a notação aditiva para representar a operação binária do monóide S. Escreveremos apenas S para representar o semigrupo $(S,+)$.

Definição 1.1.2. *Um semigrupo S diz-se **comutativo** se a operação $+$ for comutativa, i.e, se*

$$\forall a,b,c \in S\colon\ a+b = b+a.$$

Definição 1.1.3. *Diz-se que $e \in S$ é **elemento identidade** de S se:*

$$\forall a \in S,\ a + e = e + a = a.$$

Proposição 1.1.1. *Num semigrupo S , se existir, o elemento identidade é único.*

Demonstração. *Suponhamos que S tem dois elementos identidade e_1 e e_2. Por um lado, como e_1 é identidade de S, temos $e_1 + e_2 = e_2$. Por outro lado, como e_2 é identidade de S, obtemos $e_1 + e_2 = e_1$. Logo $e_1 = e_2$. Assim, um semigrupo tem, no máximo um elemento identidade.*

■

Quando existe, o elemento identidade de S representa-se por 0_S ou, caso não haja ambiguidade, apenas por 0.

Associada à estrutura de semigrupo, surge a noção de monóide.

Definição 1.1.4. *Um **monóide** é um semigrupo S com identidade.*

Exemplos:

1. O semigrupo $(2\mathbb{N}, \cdot)$ não tem identidade.
2. $(\mathbb{N}_0, +)$ é um monóide com identidade 0.
3. $(\mathbb{Z}, \times)$ é um monóide com identidade 1.
4. $(M_{n\times p}(\mathbb{R}), +)$ é um monóide cuja identidade é a matriz nula $O_{n\times p}$.
5. $(F(X), \circ)$, em que X é um conjunto, $F(X)$ representa o conjunto das funções de X em X e $\circ$ é a composição de funções, é um monóide cuja identidade é a função id_X.

No capítulo 3 estudaremos uma classe de semigrupos que satisfazem a chamada lei do corte. Diz-se que um semigrupo S satisfaz a **lei do corte** se

$$\forall x, y, z \in S:\ x + z = y + z \Rightarrow x = y \ \wedge\ z + x = z + y \Rightarrow x = y.$$

A lei do corte não é necessariamente satisfeita num semigrupo arbitrário. De facto, no semigrupo $(F(\mathbb{N}), \circ)$, as aplicações $f,\ g\ e\ h \in F(\mathbb{N})$ definidas por $f(x) = 2,\ g(x) = 2x$ e $h(x) = 2x + 1$, para qualquer $x \in \mathbb{N}$, são tais que $f \circ g = f \circ h$. No entanto, $g \neq h$.

Definição 1.1.5. *Um semigrupo diz-se* ***cancelativo*** *se a operação nele definida satisfaz a lei do corte.*

Definição 1.1.6. *Seja S um monóide. Um elemento $b \in S$ diz-se um* ***simétrico de*** *$a \in S$ se satisfaz a condição $a+b=b+a=0$.*

Proposição 1.1.2. *Seja S um monóide. Então, cada elemento $a \in S$ tem, no máximo, um elemento simétrico.*

Demonstração. *Seja $a \in S$. Suponhamos que $b, c \in S$ são simétricos de a. Então:*

$$b = b+0 = b+(a+c) = (b+a)+c = 0+c = c.$$

■

Num monóide S, o simétrico de $a \in S$, se existir, representa-se por $-a$.

Definição 1.1.7. *Seja S um monóide. Um subconjunto H de S diz-se um* ***submonóide*** *de S se:*

- $0 \in H$
- $\forall a, b \in H,\ a+b \in H$.

Proposição 1.1.3. *A interseção de uma família $\{S_i\}_{i\in I}$ de submonóides de um monóide S é um submonóide de S.*

Demonstração. *Sejam I um conjunto não vazio de índices e $\{S_i\}_{i\in I}$ uma família de submonóides de S. Como $S_i \subseteq S$, qualquer que seja $i \in I$, é claro que $\bigcap_{i\in I} S_i \subseteq S$. Para além disso, uma vez que, para qualquer $i \in I$ se tem $0 \in S_i$, a definição de interseção de conjuntos garante que $0 \in \bigcap_{i\in I} S_i$. Finalmente, sejam $a, b \in \bigcap_{i\in I} S_i$. Então $a,\ b \in S_i$, para qualquer $i \in I$ e, uma vez que todo o S_i é um submonóide de S, obtemos $a+b \in S_i$, para qualquer $i \in I$. Logo $a+b \in \bigcap_{i\in I} S_i$. Assim, $\bigcap_{i\in I} S_i$ é um submonóide de S.*

■

Sejam S um monóide e $A \subseteq S$. Seja $\{S_i\}_{i\in I}$ a família de todos os submonóides de S que contêm A. Pela Proposição 1.1.3, $\bigcap_{i\in I} S_i$ é um submonóide de S. Além disso, como $A \subseteq S_i$, para qualquer

$i \in I$, temos $A \subseteq \bigcap_{i\in I} S_i$. Finalmente, se M é um submonóide de S e $A \subseteq M$ então $M = S_j$, para algum $j \in I$ e, portanto, $\bigcap_{i\in I} S_i \subseteq M$. Temos, assim, que $\bigcap_{i\in I} S_i$ é o menor submonóide de S que contém A. Deste modo, faz sentido introduzir a seguinte definição:

Definição 1.1.8. *Dado um monóide S e um subconjunto A de S, chama-se **submonóide de** S **gerado por** A e, representa-se por $\langle A\rangle$, ao menor submonóide de S que contém A.*

Como veremos mais adiante, é importante conhecermos a 'forma' dos elementos de $\langle A\rangle$. Para tal, precisamos de introduzir o conceito de *múltiplo-n* de um elemento de S, para qualquer $n \in \mathbb{N}_0$.

Definição 1.1.9. *Sejam S um monóide, $a \in S$ e $n \in \mathbb{N}_0$. Chama-se **múltiplo-n** de a e representa-se por na ao elemento de S assim definido:*

- $0a = 0$;
- $(n+1)a = na + a$, *para qualquer* $n \in \mathbb{N}_0$.

Proposição 1.1.4. *Sejam S um monóide, $a, b \in S$ e $n, p \in \mathbb{N}_0$. Então:*

i) $n(a+b) = na + nb$;

ii) $(np)a = n(pa) = p(na)$.

Proposição 1.1.5. *Sejam S um monóide e A um subconjunto de S. Então:*

$$\langle A\rangle = \left\{ \sum_{i=1}^{r} n_i a_i : \ r \in \mathbb{N},\ n_i \in \mathbb{N} \text{ e } a_i \in A, \text{ para qualquer } 1 \le i \le r \right\}$$

Demonstração. *Seja* $\mathcal{T} = \left\{ \sum_{i=1}^{r} n_i a_i : \ r \in \mathbb{N},\ n_i \in \mathbb{N} \text{ e } a_i \in A, \text{ para qualquer } 1 \le i \le r \right\}$. *Como, para cada $a \in A$, $a = 1a$, é claro que $A \subseteq \mathcal{T}$. Cálculos de rotina mostram que $\mathcal{T}$ é submonóide de S. Finalmente, se M é um submonóide de S que contém A, então, dado $x = \sum_{i=1}^{r} n_i a_i \in \mathcal{T}$, temos que $a_i \in M$ e $n_i a_i \in M$, para qualquer i. Logo $\sum_{i=1}^{r} n_i a_i \in M$, isto é, $x \in M$. Assim, $\mathcal{T} \subseteq M$. Portanto, $\mathcal{T} = \left\{ \sum_{i=1}^{r} n_i a_i : \ r \in \mathbb{N}, n_i \in \mathbb{N}, a_i \in A, 1 \le i \le r \right\}$ é o menor submonóide de S que contém A.*

■

Quando, para certo $A \subseteq S$, $S = \langle A \rangle$, dizemos que S é gerado por A ou que A é um **conjunto de geradores** de S. Tem-se sempre que $S = \langle S \rangle$, para qualquer monóide S.

Definição 1.1.10. *Um monóide S diz-se **finitamente gerado** se admite um conjunto finito de geradores.*

O produto cartesiano de n monóides, com $n \in \mathbb{N}$, pode ser algebrizado de modo muito natural com o objetivo de se obter um novo monóide. Vejamos como.

Sejam $n \in \mathbb{N}$ e $S_1, S_2, ..., S_n$ n monóides. Consideremos o produto cartesiano $S_1 \times S_2 \times .... \times S_n$. Para quaisquer $(a_1, a_2, ..., a_n)$ e $(b_1, b_2, ..., b_n) \in S_1 \times S_2 \times .... \times S_n$ definimos

$$(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n).$$

Cálculos simples mostram que a seguinte proposição é verdadeira.

Proposição 1.1.6. *Sejam $n \in \mathbb{N}$ e $S_1, ..., S_n$ n monóides. O conjunto $S_1 \times S_2 \times ... \times S_n$ munido da operação definida anteriormente é um monóide.*

Definição 1.1.11. *O monóide $(S_1 \times S_2 \times ... \times S_n, +)$ designa-se por **produto direto** de $S_1, S_2, ..., S_n$. Se $S_i = S_j = T$ para todo $1 \leq i \leq n$, o produto direto $(S_1 \times S_2 \times ... \times S_n, +)$ representa-se por T^n.*

Definição 1.1.12. *Um monóide S diz-se um **grupo** se todos os elementos de S admitirem simétrico.*

Definição 1.1.13. *Sejam S um grupo e $H \subseteq S$. Diz-se que H é um **subgrupo** de S se $(H, +|_H)$ é um grupo. Escreve-se $H < S$ para representar que H é um subgrupo de S.*

Proposição 1.1.7. *Sejam S um grupo e $H \subseteq S$. H é um subgrupo de S se e só se:*

i) $0 \in H$;

ii) se $x, y \in H$ *então* $x - y \in H$.

Demonstração. *Suponhamos que $(H, +|_H)$ é grupo. Então, $H \neq \varnothing$ e podemos, portanto, tomar $x \in H$ e considerar $-x \in H$. Como, $x + (-x) \in H$, obtemos $0 \in H$. Dados $x, y \in H$, como $(H, +|_H)$ é grupo, temos que, $-y \in H$ e que $x + (-y) \in H$, i.e, ii) é satisfeita.*

Reciprocamente, suponhamos i) e ii) satisfeitas. Tomemos $y \in H$. Como $0 \in H$, por ii), obtemos então $0 - y \in H$, i.e., $-y \in H$. Além disso, se $x \in H$, por ii) obtemos $x - (-y) \in H$, i.e, $x + y \in H$. Logo $(H, +|_H)$ é subgrupo de $(S, +)$. ■

Proposição 1.1.8. *Todo o grupo é um monóide cancelativo.*

Demonstração. *Seja S um grupo. Por definição de grupo, S é um monóide. Sejam* $a,\ b,\ c \in S$. *Temos:*

$$\begin{aligned} a+b=a+c &\Rightarrow -a+(a+b)=-a+(a+c) \\ &\Rightarrow (-a+a)+b=(-a+a)+c \qquad (propriedade\ associativa) \\ &\Rightarrow 0+b=0+c \\ &\Rightarrow b=c \end{aligned}$$

Analogamente, $a+b=c+b \Rightarrow a=c$.

■

Seguindo um procedimento análogo ao estabelecido para os monóides, prova-se que, dado um grupo G e um subconjunto X de G, a intersecção de todos os subgrupos de G que contêm X é o menor subgrupo de G que contém X. Este subgrupo representa-se por $\langle X \rangle$ e designa-se por ***subgrupo de*** G ***gerado por*** X. Uma vez que, num grupo existe identidade e todos os elementos têm simétrico, o conceito de *múltiplo-n* de um elemento de um monóide $n \in \mathbb{N}_0$ pode ser estendido para qualquer inteiro:

Definição 1.1.14. *Sejam G um grupo ,* $a \in G$ *e* $n \in \mathbb{Z}$. *Chama-se* ***múltiplo-n*** *de a, e representa-se por na, ao elemento de G assim definido:*

- $0a = 0$
- $(n+1)a = na + a,\ se\ n \in \mathbb{N}_0$
- $na = -(-na),\ se\ n \in \mathbb{Z}^-$.

Uma proposição análoga à Proposição 1.1.4 é válida para qualquer grupo G e quaisquer inteiros n e p.

Proposição 1.1.9. *Sejam S um monóide,* $a,\ b \in S$ *e* $n,\ p \in \mathbb{Z}$. *Então:*

i) $n(a+b) = na + nb$;

ii) $(np)a = n(pa) = p(na)$.

Com uma argumentação em tudo semelhante à usada na demonstração da Proposição 1.1.5 prova-se que a seguinte proposição é verdadeira:

Proposição 1.1.10. *Dado um grupo G e um subconjunto X de G,*

$$\langle X\rangle = \left\{ \sum_{i=1}^{r} z_i a_i : \ r \in \mathbb{N},\ z_i \in \mathbb{Z} \ \ e \ \ a_i \in A,\ \textit{para qualquer } 1 \leq i \leq r. \right\}$$

Se $G = X$ e X é finito, diz-se que G é **finitamente gerado**.

Tendo em conta o modo como a operação de adição está definida em $S_1 \times S_2 \times \ldots \times S_n$, cálculos simples mostram que há propriedades algébricas dos monóides $S_1, \ldots, S_n$ que são "herdadas" pelo monóide $S_1 \times S_2 \times \ldots \times S_n$.
Temos, assim, a seguinte proposição:

Proposição 1.1.11. *Sejam $n \in \mathbb{N}$ e $S_1, \ldots, S_n$ n monóides. Então,*

i) Se os monóides $S_1, \ldots, S_n$ são cancelativos então $S_1 \times S_2 \times \ldots \times S_n$ é cancelativo.

ii) Se os monóides $S_1, \ldots, S_n$ são finitamente gerados então $S_1 \times S_2 \times \ldots \times S_n$ é finitamente gerado.

iii) Se os monóides $S_1, \ldots, S_n$ são grupos então $S_1 \times S_2 \times \ldots \times S_n$ é um grupo.

1.2 Congruências

Em toda esta secção $(S, +)$ é um monóide que representaremos apenas por S.
Uma relação binária em S é um subconjunto de $S \times S$. Dados uma relação binária σ em S e $a,\ b \in S$, escreveremos $a\sigma b$ para indicar que $(a, b) \in \sigma$.

Definição 1.2.1. *Uma relação binária σ definida em S diz-se uma **relação de equivalência** em S se satisfaz as seguintes propriedades:*

- *é reflexiva: $\forall a \in S,\ a\sigma a$;*
- *é simétrica: se $a\sigma b$ então $b\sigma a$, para quaisquer $a, b \in S$;*
- *é transitiva : se $a\sigma b$ e $b\sigma c$ então $a\sigma c$, para quaisquer $a,\ b,\ c \in S$.*

Sendo σ uma relação de equivalência definida em S, representamos por $\overline{a}$ ou por $[a]_\sigma$, $(a \in S)$ a classe de equivalência de a determinada por σ, $\overline{a} = \{b \in S : a\sigma b\}$, e por S/σ o conjunto quociente determinado por σ: $S/\sigma = \{\overline{a} : a \in S\}$.

Definição 1.2.2. *Uma relação de equivalência σ em S diz-se uma **congruência** se é compatível com a operação + de S, isto é, se, para quaisquer $a,\ b, c\ \in S$*

$$a\sigma b \Rightarrow (a+c)\sigma(b+c)\ e\ (c+a)\sigma(c+b). \qquad (1)$$

Cálculos algébricos simples mostram que a condição (1) é equivalente à condição:

$$a\sigma b \wedge c\sigma d \Rightarrow (a+c)\,\sigma\,(b+d)\ e\ (c+a)\,\sigma\,(d+b)$$

Seja σ uma relação de congruência em *S*. Verificamos de seguida que o facto de σ ser compatível com a operação + permite definir em S/σ uma operação de adição à custa da adição em *S*. Definamos

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad (2)$$

para quaisquer $a,\ b \in S$ e mostremos que esta igualdade define uma operação em S/σ, i.e, que o resultado $\overline{a+b}$ não depende da escolha do representante em cada uma das classes $\overline{a}$ e $\overline{b}$. Sejam $x \in \overline{a}$ e $y \in \overline{b}$. Temos:

$$x \in \overline{a} \text{ e } y \in \overline{b} \Rightarrow x\sigma a \text{ e } y\sigma b \Rightarrow (x+y)\,\sigma\,(a+b) \Rightarrow \overline{x+y} = \overline{a+b}.$$

Assim, $\overline{x} + \overline{y} = \overline{x+y} = \overline{a+b} = \overline{a} + \overline{b}$.

Cálculos rotineiros, assentes na Definição 1.2.2, mostram que a adição em S/σ "herda"as propriedades da adição em *S*.

Proposição 1.2.1. *Sejam S um monóide comutativo e σ uma congruência definida em S. Então o conjunto, S/σ munido da operação definida em (2), é um monóide comutativo.*

Ao monóide $(S/\sigma, +)$ dá-se o nome de **monóide quociente de** *S* **determinado por** σ, que representaremos apenas por S/σ.

Proposição 1.2.2. *Sejam S um monóide e σ uma congruência definida em S. Temos que:*

i) Se S é um grupo então S/σ também é um grupo;

ii) Se S é finitamente gerado então S/σ também é finitamente gerado.

Demonstração. *i) Sendo 0_S a identidade de S, temos que $\overline{0_S}$ é a identidade de S/σ e, para cada, $\overline{a} \in S/\sigma$, $-\overline{a} = \overline{-a}$.*

ii) Sendo $S = \langle A \rangle$, onde $A = \{a_1, ..., a_n\}$, $n \in \mathbb{N}$, temos que $S/\sigma = \langle B \rangle$, onde $B = \{\overline{a_1}, ..., \overline{a_n}\}$, sendo possível que $\overline{a_i} = \overline{a_j}$ para $i \neq j$. Assim, o número de geradores de S/σ é menor ou igual a n e S/σ é, portanto, finitamente gerado.

■

1.3 Morfismos

Nesta secção, S e S' são monóides.

Definição 1.3.1. *Diz-se que uma aplicação $f : S \to S'$ é um **morfismo de monóides** se:*

- $f(0_S) = 0_{S'}$;
- $\forall a, b \in S, \quad f(a+b) = f(a) + f(b)$.

Se a aplicação f satisfaz apenas a segunda condição, diz-se que f é um morfismo de semigrupos ou, apenas, que f é um morfismo.

Um morfismo de monóides $f : S \to S'$ diz-se um:

- **monomorfismo** se f é injetiva;
- **epimorfismo** se f é sobrejetiva;
- **isomorfismo** se f é bijetiva.

Sejam S e S' semigrupos (respetivamente monóides). Se existir um isomorfismo de semigrupos (respetivamente monóides), $f : S \to S'$, diz-se que S é isomorfo a S' e escreve-se $S \simeq S'$.

Uma vez que a aplicação inversa de um isomorfismo é ainda um isomorfismo, se $S \simeq S'$ então $S' \simeq S$. Assim, sem ambiguidade, dizemos que dois monóides são isomorfos se existe um isomorfismo entre eles.

Proposição 1.3.1. *Sejam S e S' dois monóides isomorfos. Então:*

i) S é um monóide cancelativo se e só se S' é cancelativo;

ii) S é um monóide finitamente gerado se e só se S' é finitamente gerado.

Demonstração. *Sejam S e S' monóides e $f : S \to S'$ um isomorfismo de monóides.*

i) Sejam a', b' e c' elementos quaisquer de S' que satisfazem $a' + b' = c' + b'$ e sejam $a, b, c \in S$, tais que $f(a) = a'$, $f(b) = b'$ e $f(c) = c'$. Então

$$\begin{aligned} a' + b' = c' + b' &\Leftrightarrow f(a) + f(b) = f(c) + f(b) \\ &\Leftrightarrow f(a + b) = f(c + b) \\ &\Leftrightarrow a + b = c + b \\ &\Leftrightarrow a = c \\ &\Leftrightarrow f(a) = f(c) \\ &\Leftrightarrow a' = c'. \end{aligned}$$

ii) Temos $S = \langle s_1 \ s_2 \ \dots \ s_n \rangle \Leftrightarrow f(S) = \langle f(s_1) \ f(s_2) \ \dots \ f(s_n) \rangle \Leftrightarrow S' = \langle f(s_1) \ f(s_2) \ \dots \ f(s_n) \rangle$

■

Definição 1.3.2. *Seja $f : S \to S'$ um morfismo de monóides. Chama-se **núcleo** de f, e representa-se por $Nuc\, f$, à relação binária assim definida:*

$$Nuc\, f = \{(a, b) \in S \times S : f(a) = f(b)\}.$$

A relação $Nuc f$ é uma relação de equivalência e, por f ser um morfismo, $Nuc f$ é também compatível com a adição:

$$\begin{aligned} f(a) = f(b) \text{ e } f(c) = f(d) &\Rightarrow f(a) + f(c) = f(b) + f(d) \\ &\Leftrightarrow f(a+c) = f(b+d) \\ &\Leftrightarrow (a+c, b+d) \in Nuc f. \end{aligned}$$

Assim,

Proposição 1.3.2. *Seja $f : S \to S'$ um morfismo de monóides. A relação binária $Nuc f$ é uma congruência em S.*

Definição 1.3.3. *Seja $f : S \to S'$ um morfismo de monóides. Chama-se* ***imagem da aplicação*** *f e representa-se por $Im(f)$ ao contradomínio de f:*

$$Im(f) = \{ f(a) : a \in S \}.$$

Proposição 1.3.3. *Seja $f : S \to S'$ um morfismo de monóides. O par $(Im(f), +)$ é um submonóide de S'.*

Demonstração. *Como f é morfismo de monóides, $f(0_S) = 0_{S'}$ e, portanto, $0_{S'}$ pertence a $Im(f)$. Logo $Im(f) \neq \varnothing$. Por outro lado, se $a', b' \in Im f$ então $a' = f(a)$ e $b' = f(b)$ para certos $a, b \in S$. Assim, $a' + b' = f(a) + f(b) = f(a+b)$ e, portanto, $a' + b' \in Im f$.*

■

Estamos agora em condições de estabelecer o Teorema do Homomorfismo para monóides.

Teorema 1.3.1. *Seja $f : S \to S'$ um morfismo de monóides. Então a aplicação $\overline{f} : S/Nuc f \to Im f$, definida por $\overline{f}(\overline{a}) = f(a)$, é um isomorfismo de monóides.*

Demonstração. *A aplicação $\overline{f}$ é trivialmente sobrejetiva. É também, injetiva: para quaisquer $\overline{a}, \overline{b} \in S/Nuc f$, tem-se*

$$\overline{f}(\overline{a}) = \overline{f}(\overline{b}) \Leftrightarrow f(a) = f(b) \Leftrightarrow (a,b) \in Nuc f \Rightarrow \overline{a} = \overline{b}.$$

Finalmente, $\overline{f}$ é um morfismo de monóides. De facto, por um lado, por definição de $\overline{f}$, $\overline{f}(\overline{0}) = f(0_S)$ e, como f é morfismo de monóides, $f(0_S) = 0_{S'}$, pelo que $\overline{f}(\overline{0}) = 0_{S'}$. Por outro lado, para quaisquer $\overline{a}, \overline{b} \in S/Nuc\, f$, tem-se

$$\overline{f}\left(\overline{a}+\overline{b}\right) = \overline{f}\left(\overline{a+b}\right) = f(a+b) = f(a) + f(b) = \overline{f}(\overline{a}) + \overline{f}\left(\overline{b}\right).$$

■

1.4 Monóides finitamente gerados

Proposição 1.4.1. *Seja S um monóide gerado por n elementos $s_1, s_2, \ldots, s_n$. Então existe uma congruência σ definida em $\mathbb{N}^n$ tal que S é isomorfo a $\mathbb{N}^n/\sigma$.*

Demonstração. *Dados os monóides $\mathbb{N}^n$ e $S = \langle s_1, \ldots, s_n \rangle$, consideremos a aplicação $f : \mathbb{N}^n \to S$ definida por $f(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i s_i$, para qualquer $(a_1, \ldots, a_n) \in \mathbb{N}^n$. Cálculos simples mostram que f é um morfismo de monóides. A aplicação f é também sobrejetiva uma vez que, sendo $S = \langle s_1, \ldots, s_n \rangle$, qualquer $b \in S$ é tal que $b = \sum_{i=1}^{n} b_i s_i$ para certos $b_1, b_2, \ldots, b_n \in \mathbb{N}$. Assim, $b = f(b_1, \ldots, b_n)$.*

Consideremos agora $\sigma = Nuc\, f$. Pela Proposição 1.3.2, σ é uma congruência em $\mathbb{N}^n$ e, pelo Teorema 1.3.1, $\mathbb{N}^n/Nuc\, f \simeq Im\, f$. Como f é sobrejetiva, segue-se que S é isomorfo a $\mathbb{N}^n/Nuc\, f$.

■

Em vista deste teorema, estudar propriedades dos monóides finitamente gerados é, de algum modo, estudar propriedades das congruências em $\mathbb{N}^n$. A Proposição 1.4.5 ilustra esta situação.

Seja σ uma congruência definida em $\mathbb{N}^n$. Consideremos o seguinte subconjunto de $\mathbb{Z}^n$:

$$M_\sigma = \{a - b : a, b \in \mathbb{N}^n \wedge (a, b) \in \sigma\}.$$

Proposição 1.4.2. *Seja σ uma congruência definida em $\mathbb{N}^n$. O conjunto M_σ é um subgrupo de $\mathbb{Z}^n$.*

Demonstração. *Seja $M_\sigma = \{a - b : a, b \in \mathbb{N}^n \wedge (a, b) \in \sigma\} \subseteq \mathbb{Z}^n$. Temos:*

- $M_\sigma \neq \varnothing$

Como σ é reflexiva, $(a,a) \in \sigma$, para qualquer $a \in \mathbb{Z}^n$ e, portanto $a-a \in M_\sigma$. Logo $0 \in M_\sigma$. Assim, $M_\sigma \neq \emptyset$.

- *Se $a-b,\ x-y \in M_\sigma$, então $(a-b)+(x-y) \in M_\sigma$*

$$\begin{aligned} a-b,\ x-y \in M_\sigma &\Rightarrow (a,b),(x,y) \in \sigma \\ &\Rightarrow (a+x,b+y) \in \sigma \\ &\Rightarrow (a+x)-(b+y) \in M_\sigma \\ &\Leftrightarrow (a-b)+(x-y) \in M_\sigma. \end{aligned}$$

- $a-b \in M_\sigma \Rightarrow -(a-b) \in M_\sigma$

  De $a-b \in M_\sigma$ obtemos $(a,b) \in \sigma$. Como σ é simétrica, $(b,a) \in \sigma$, isto é, $b-a \in M_\sigma$. Então $-(a-b) \in M_\sigma$.

■

A cada congruência de $\mathbb{N}^n$ está, assim, associado um subgrupo de $\mathbb{Z}^n$. Podemos pensar agora na situação recíproca: dado um subgrupo H de $\mathbb{Z}^n$ definimos uma relação binária associada a este subgrupo.

Definição 1.4.1. *Seja H um subgrupo de $\mathbb{Z}^n$. Representa-se por $\sim_H$ a relação binária definida em $\mathbb{N}^n$ por:*

$$\sim_H = \{(a,b) \in \mathbb{N}^n \times \mathbb{N}^n : a-b \in H\}.$$

Proposição 1.4.3. *Seja H um subgrupo de $\mathbb{Z}^n$. A relação binária $\sim_H$ definida em 1.4.1 é uma congruência em $\mathbb{N}^n$.*

Demonstração. *Claramente $\sim_H$ é uma relação de equivalência em $\mathbb{N}^n$. De facto, para qualquer $a \in H$, $a-a \in H$ porque H é subgrupo de $\mathbb{Z}^n$ e, portanto $(a,a) \in \sim_H$. Também por H ser subgrupo de $\mathbb{Z}^n$, se $a-b \in H$ então $-(a-b) = -a+b \in H$, isto é, $(b,a) \in \sim_H$. Finalmente, se $a-b \in H$ e $b-c \in H$ então $(a-b)+(b-c) \in H$, isto é, $a-c \in H$, ou seja $(a,c) \in \sim_H$. Tomemos agora $(a,b),(c,d) \in \sim_H$. Temos, então, $a-b \in H$ e $c-d \in H$ pelo que, por H ser subgrupo de $\mathbb{Z}^n$, obtemos*

$(a-b)+(c-d) \in H$. *A associatividade e a comutatividade da operação de adição permitem concluir que* $(a+c)-(b+d) \in H$, *isto é, que* $(a+c, b+d) \in \sim_H$.

■

Mostrámos, assim, que cada subgrupo de $\mathbb{Z}^n$ determina uma congruência em $\mathbb{N}^n$.

Sendo σ uma congruência em $\mathbb{N}^n$ e H um subgrupo de $\mathbb{Z}^n$, uma vez que M_σ é um subgrupo de $\mathbb{Z}^n$ e $\sim_H$ é uma congruência em $\mathbb{N}^n$, colocam-se agora duas questões:

1. Será que $\sim_{M_\sigma} = \sigma$?
2. Será que $M_{\sim_H} = H$?

À questão 2. é simples responder. De facto, por um lado, se $x \in M_{\sim_H}$ então $x = a - b$, para algum $(a,b) \in \sim_H$. Por definição de $\sim_H$, isto é equivalente a dizer que $a - b \in H$ e, portanto, $x \in H$. Por outro lado, dado $x \in H$, como $x = x - 0$, obtemos $(x,0) \in \sim_H$ e, portanto, $x \in M_{\sim_H}$. Assim, $M_{\sim_H} = H$.

Relativamente à primeira questão, mostramos de seguida que a igualdade $\sim_{M_\sigma} = \sigma$ nem sempre é válida.

Proposição 1.4.4. *Seja* σ *uma congruência definida em* $\mathbb{N}^n$. *Então:*

i) $\sigma \subseteq \sim_{M_\sigma}$;

ii) $\forall (a,b) \in \sim_{M_\sigma} \ \exists c \in \mathbb{N}^n : (a+c, b+c) \in \sigma$.

Demonstração. *i) Sejam* $a, b \in \mathbb{N}^n$. *Atendendo à definição de* M_σ *e de* $\sim_{M_\sigma}$, *temos:*

$$(a,b) \in \sigma \Rightarrow a - b \in M_\sigma \Rightarrow (a,b) \in \sim_{M_\sigma},$$

o que garante que $\sigma \subseteq \sim_{M_\sigma}$.

ii) Se $(a,b) \in \sim_{M_\sigma}$ *então* $a - b \in M_\sigma$ *e, portanto,* $a - b = x - y$, *para algum* $(x,y) \in \sigma$. *Como* σ *é uma congruência em* $\mathbb{N}^n$ *e* $a \in \mathbb{N}^n$, *de* $(x,y) \in \sigma$ *obtemos* $(a+x, a+y) \in \sigma$ *e, uma vez que* $a + y = b + x$, *concluimos que* $(a+x, b+x) \in \sigma$. *Fazendo* $x = c$, *temos* $(a+c, b+c) \in \sigma$.

■

O próximo resultado mostra que a igualdade $\sim_{M_\sigma} = \sigma$ está relacionada com a "cancelatividade" do monóide $\mathbb{N}^n/\sigma$.

Proposição 1.4.5. *Para qualquer congruência σ definida em $\mathbb{N}^n$, tem-se que $\sigma = \sim_{M_\sigma}$ se e só se o monóide $\mathbb{N}^n/\sigma$ é cancelativo.*

Demonstração. *Seja σ uma congruência definida em $\mathbb{N}^n$. Suponhamos que $\sigma = \sim M_\sigma$ e sejam $\overline{a}, \overline{b}$, e $\overline{c} \in \mathbb{N}^n/\sigma$ tais que $\overline{a}+\overline{c} = \overline{b}+\overline{c}$. Então, $\overline{a+c} = \overline{b+c}$, isto é, $(a+c)\,\sigma\,(b+c)$. Pela Proposição 1.4.4 i), obtemos $(a+c) \sim_{M_\sigma} (b+c)$, isto é, $(a+c)-(b+c) \in M_\sigma$. Então $a+c-b-c \in M_\sigma$, ou seja, $a-b \in M_\sigma$ e, portanto, $(a,b) \in \sigma$. Assim, $\overline{a} = \overline{b}$ o que permite concluir que $\mathbb{N}^n/\sigma$ é cancelativo.*

Admitamos agora que o monóide $\mathbb{N}^n/\sigma$ é cancelativo. Pretendemos mostrar que $\sigma = \sim_{M_\sigma}$. Por um lado, tendo em atenção a Proposição 1.4.4, temos $\sigma \subseteq \sim_{M_\sigma}$. Por outro lado, se $(a,b) \in \sim_{M_\sigma}$, a Proposição 1.4.4 garante a existência de um elemento $c \in \mathbb{N}^n$ tal que $(a+c, b+c) \in \sigma$. Temos:

$$\overline{a+c} = \overline{b+c} \quad \Rightarrow \overline{a}+\overline{c} = \overline{b}+\overline{c}$$

e, como $\mathbb{N}^n/\sigma$ é cancelativo, segue-se que $\overline{a} = \overline{b}$. Logo $(a,b) \in \sigma$.

■

Como vimos, a cada subgrupo de $\mathbb{Z}^n$ está associada uma congruência $\sim_H$ definida em $\mathbb{N}^n$ por:

$$a \sim_H b \Leftrightarrow a-b \in H, \text{ para quaisquer } a,\ b \in \mathbb{N}^n.$$

Sabemos, da Teoria de Grupos, que cada subgrupo H de um grupo abeliano G (no nosso caso, $\mathbb{Z}^n$) determina uma congruência no grupo, nomeadamente a congruência $\equiv (\bmod H)$ definida em $\mathbb{Z}^n$ por:

$$a,\ b \in \mathbb{Z}^n,\ a \equiv b\,(\bmod H) \Leftrightarrow a-b \in H.$$

O monóide quociente $\mathbb{Z}^n/\bmod H$ é um grupo que é representado por $\mathbb{Z}^n/H$.

O próximo resultado relaciona as congruências $\sim_H$ e $\equiv (\bmod H)$.

Proposição 1.4.6. *Seja H um subgrupo de $\mathbb{Z}^n$. A correspondência $i : \mathbb{N}^n/\sim_H \to \mathbb{Z}^n/H$ tal que $i(\overline{a}_{\sim_H}) = \overline{a}_{\equiv_H}$ é um monomorfismo de monóides.*

Demonstração. *Comecemos por verificar que a correspondência i é uma aplicação. De facto, se $\overline{a}_{\sim_H} = \overline{b}_{\sim_H} \in \mathbb{N}^n/\sim_H$ então $a,b \in \mathbb{N}^n$ e $(a,b) \in \sim_H$. Logo, $a,b \in \mathbb{Z}^n$ e $a-b \in H$ o que significa que $a \equiv b\,(\bmod H)$.*

- *A aplicação i é injetiva. Sejam* $\overline{a}_{\sim_H}, \overline{b}_{\sim_H} \in \mathbb{N}^n/\sim_H$ *tais que* $\overline{a}_{\equiv \bmod H} = \overline{b}_{\equiv \bmod H}$. *Então* $a - b \in H$. *Como* $a,\ b \in \mathbb{N}^n$, *obtemos* $(a,b) \in \sim_H$, *isto é,* $\overline{a}_{\sim_H} = \overline{b}_{\sim_H}$.

- *A aplicação i é um morfismo de monóides.*

  Por definição de i, $i\left(\overline{0}_{\sim_H}\right) = \overline{0}_{\equiv(\bmod H)}$. *Por outro lado, dados* $\overline{a}_{\sim_H}$, $\overline{b}_{\sim_H} \in \mathbb{N}^n/\sim_H$, *temos*

$$\begin{aligned} i\left(\overline{a}_{\sim_H} + \overline{b}_{\sim_H}\right) &= i\left(\overline{a_{\sim_H} + b_{\sim_H}}\right) \\ &= \overline{a+b}_{\equiv(\bmod H)} \\ &= \overline{a}_{\equiv(\bmod H)} + \overline{b}_{\equiv(\bmod H)} \\ &= i\left(\overline{a}_{\sim_H}\right) + i\left(\overline{b}_{\sim_H}\right). \end{aligned}$$

■

Uma vez que qualquer monóide *S*, gerado por *n* elementos ($n \in \mathbb{N}$), é isomorfo a um monóide quociente $\mathbb{N}^n/\sigma$, para certa congruência σ de $\mathbb{N}^n$ (Proposição 1.4.1), se *S* é cancelativo então $\mathbb{N}^n/\sigma$ é também cancelativo (Proposição 1.3.1) e, portanto, obtemos, pela Proposição 1.4.5, que um monóide finitamente gerado (*n* geradores) é cancelativo se e só se é isomorfo a um monóide quociente $\mathbb{N}^n/\sim_{M_\sigma}$ para alguma congruência σ de $\mathbb{N}^n$.

Temos, portanto, o seguinte corolário:

Corolário 1.4.1. *Seja S um monóide finitamente gerado. Então S é cancelativo se e só se S é isomorfo a um submonóide de um grupo.*

Uma classe importante de monóides cancelativos é a classe dos grupos.

Definição 1.4.2. *Seja a um elemento qualquer de* $\mathbb{Z}^n$. *Diz-se que:*

- *a é* ***fortemente positivo*** *se todas as suas coordenadas, em relação a uma qualquer base de* $\mathbb{Z}^n$, *são positivas;*

- *a é* ***não negativo*** *se todas as suas coordenadas, em relação a uma qualquer base de* $\mathbb{Z}^n$, *são não negativas.*

Proposição 1.4.7. *Seja S um monóide finitamente gerado. As afirmações seguintes são equivalentes:*

i) S é um grupo;

ii) S é isomorfo a $\mathbb{N}^n/\sim_H$ *para algum número positivo n e algum subgrupo H de* $\mathbb{Z}^n$ *que contém um elemento fortemente positivo;*

iii) S é isomorfo a $\mathbb{Z}^n/H$ *para algum número positivo n e algum subgrupo H de* $\mathbb{Z}^n$.

Demonstração. *Seja S um monóide finitamente gerado.*

- $i) \Rightarrow ii)$

  Como S é grupo, S é, em particular, um monóide cancelativo e, portanto, da prova do Corolário 1.4.1, temos que S é isomorfo a $\mathbb{N}^n/\sim_{M_\sigma}$ *para algum número inteiro positivo n e para alguma congruência* σ *definida em* $\mathbb{N}^n$. *Dado que S é um grupo,* $\mathbb{N}^n/\sim_{M_\sigma}$ *também é um grupo e, por isso, o elemento* $\overline{(1,\ldots,1)}_{\sim_{M_\sigma}}$ *admite simétrico. Seja* $\overline{(a_1,\ldots,a_n)}_{\sim_{M_\sigma}}$ *o seu simétrico. Então*

  $$\overline{(a_1+1,\ldots,a_n+1)}_{\sim_{M_\sigma}} = \overline{(1,\ldots,1)}_{\sim_{M_\sigma}} + \overline{(a_1,\ldots,a_n)}_{\sim_{M_\sigma}} = \overline{(0,\ldots,0)}_{\sim_{M_\sigma}}.$$

  Logo, $(a_1+1,\ldots,a_n+1) \sim_{M_\sigma} (0,\ldots,0)$ *o que, por definição de* M_σ, *significa que* $(a_1+1,\ldots,a_n+1)-(0,\ldots,0) \in M_\sigma$. *Como,* $(a_1+1,\ldots,a_n+1)$ *é um elemento fortemente positivo de* M_σ, *a afirmação ii) é verdadeira.*

- $ii) \Rightarrow iii)$

  Sejam $a \in H$ *um elemento fortemente positivo e* $\overline{x}_{\equiv(\bmod H)}$ *um elemento arbitrário de* $\mathbb{Z}^n/H$. *Dado que todas as coordenadas de a são positivas, existe um número natural k tal que* $ka+x \in \mathbb{N}^n$. *Como* $a \in H$, *também* $ka \in H$ *e, portanto,* $\overline{ka+x}_{\equiv_H} = \overline{x}_{\equiv_H}$. *Temos*

  $$i(\overline{(ka+x)}_{\sim_H}) = \overline{(ka+x)}_{\equiv_H} = \overline{x}_{\equiv_H}$$

  o que, dada a arbitrariedade de $\overline{x}_{\equiv(\bmod H)}$, *mostra que a aplicação i (definida na Proposição 1.4.6.) é sobrejetiva. Portanto,* $\mathbb{N}^n/\sim_H \simeq \mathbb{Z}^n/H$ *e o resultado segue-se.*

- $iii) \Rightarrow i)$

  É consequência imediata do facto de $\mathbb{Z}^n/H$ *ser grupo.*

■

Capítulo 2

Grupos comutativos finitamente gerados

No capítulo anterior provámos que todo o monóide finitamente gerado é isomorfo a um monóide quociente $\mathbb{N}^n/\sigma$, para certa congruência σ de $\mathbb{N}^n$. Se, para além disso, o monóide dado for cancelativo, então ele é isomorfo a um submonóide de um grupo comutativo finitamente gerado. Por esta razão, estudamos neste capítulo, a estrutura dos grupos comutativos finitamente gerados. Veremos que o seu estudo é equivalente ao estudo de grupos quociente da forma $\mathbb{Z}^n/H$, onde H é subgrupo de $\mathbb{Z}^n$.

2.1 Base e dimensão de um subgrupo de $\mathbb{Z}^n$

Seja $n \in \mathbb{N}$ e seja $\mathbb{Z}^n$ o grupo produto direto de n fatores todos iguais a $\mathbb{Z}$ (Definição 1.1.11 e Proposição 1.1.11). Nesta secção vamos introduzir, no grupo $\mathbb{Z}^n$, conceitos semelhantes a conceitos existentes no contexto de espaço vetorial sobre um corpo. Veremos, no entanto, que nem todos os resultados relativos a espaços vetoriais são válidos no grupo $\mathbb{Z}^n$. Começamos com as duas seguintes definições.

Definição 2.1.1. *Sejam $r \in \mathbb{N}$ e $m_1, m_2, \ldots, m_r \in \mathbb{Z}^n$.*

- *Uma* **combinação linear** *de $m_1,\ m_2, \ldots, m_r$ é um elemento de $\mathbb{Z}^n$ da forma:*

$$z_1 m_1 + z_2 m_2 + \ldots + z_r m_r$$

  onde $z_i \in \mathbb{Z}$, para todo o $i \in \{1, \ldots, r\}$.

- *Os elementos* $m_1,\ m_2,\ldots,m_r$ *dizem-se* **linearmente independentes** *(escreve-se l.i.) se*

$$0_{\mathbb{Z}_n} = 0\,m_1 + 0\,m_2 + \ldots + 0\,m_r$$

for a única forma de escrever o zero de $\mathbb{Z}^n$ *como combinação linear de* $m_1, m_2, \ldots, m_r$.

Definição 2.1.2. *Sejam M um subgrupo de* $\mathbb{Z}^n$ *e* $r \in \mathbb{N}$.

- *Se* $M = \{0\}$, *chama-se* **base** *de M ao conjunto vazio.*
- *Se* $M \neq \{0\}$, *diz-se que* $\{m_1, m_2, .., m_r\} \subseteq M$ *é uma* **base** *de M se todo o elemento* $m \in M$ *se escreve de forma única como combinação linear de* $m_1, m_2, \ldots, m_r$, *isto é, na forma* $m = \sum_{i=1}^{r} z_i m_i$ *para alguns* $z_1, z_2, \ldots, z_r \in \mathbb{Z}$. *Neste caso, os elementos* $z_1,\ z_2, \ldots, z_r \in \mathbb{Z}$ *designam-se por* **coordenadas** *de m na base* $\{m_1, m_2, .., m_r\}$.

Proposição 2.1.1. *Sejam M um subgrupo de* $\mathbb{Z}^n$ *e* $r \in \mathbb{N}$. *Então* $\{m_1,\ m_2, .., m_r\}$ *é uma base de M se e só se satisfaz as seguintes condições:*

i) Todo o elemento de M pode ser escrito na forma $m = \sum_{i=1}^{r} z_i m_i$, *para alguns* $z_1,\ z_2, \ldots, z_r \in \mathbb{Z}$ *e*

ii) Se $\sum_{i=1}^{r} z_i m_i = 0$, *para alguns* $z_1,\ z_2, \ldots, z_r \in \mathbb{Z}$, *então* $z_i = 0$, *para qualquer* $i \in \{1, 2, \ldots, r\}$.

Demonstração. *Suponhamos que* $\{m_1, m_2, .., m_r\}$ *é uma base de M. A condição i) é consequência imediata da definição de base. Relativamente à condição ii), temos , por hipótese,* $\sum_{i=1}^{r} z_i m_i = 0$. *Como* $0 = 0\,m_1 + 0\,m_2 + \ldots + 0\,m_r$ *temos, como consequência da definição, que para qualquer* $i \in \{1, 2, \ldots, r\}$, $z_i = 0$.

Reciprocamente, suponhamos i) e ii). Seja $m \in M$. *Por i) temos que m se escreve na forma* $m = \sum_{i=1}^{r} z_i m_i$ *para certos* $z_1,\ z_2, \ldots, z_r \in \mathbb{Z}$. *Vamos verificar de seguida que os coeficientes* z_i *estão univocamente determinados. Suponhamos que m também se escreve na forma* $m = \sum_{i=1}^{r} z_i' m_i$, *com* $z_i' \in \mathbb{Z}$. *Temos:*

$$\sum_{i=1}^{r} z_i m_i = \sum_{i=1}^{r} z_i' m_i \Rightarrow 0 = \sum_{i=1}^{r} z_i m_i - \sum_{i=1}^{r} z_i' m_i \Rightarrow 0 = \sum_{i=1}^{r} (z_i - z_i')\, m_i.$$

Pela condição ii), obtemos, assim, $z_i - z_i' = 0$ *para qualquer* $i \in \{1,2,...,r\}$. *Portanto,* $z_i = z_i'$, *para qualquer* $i \in \{1,2,...,r\}$.

■

Sempre que $m_1, m_2, ..., m_r$ verificam a condição i), dizemos que $\{m_1, m_2, .., m_r\}$ é um **conjunto de geradores de** M e escrevemos $M = \langle m_1, m_2, ..., m_r \rangle$.

A condição ii) afirma que os elementos $m_1, m_2, ..., m_r$ de $\mathbb{Z}^n$ são linearmente independentes. Convém observar que $m_1, m_2, ..., m_r \in \mathbb{Z}^n$ são linearmente independentes se e só se são linearmente independentes como vetores do espaço vetorial $\mathbb{Q}^n$ sobre o corpo $\mathbb{Q}$.

Para cada $1 \leq i \leq n$, seja e_i o n-uplo de $\mathbb{Z}^n$ que tem a i-ésima coordenada igual a um e todas as restantes iguais a zero. É simples mostrar que $\{e_1, e_2, .., e_n\}$ é uma base de $\mathbb{Z}^n$. A esta base chama-se a **base canónica** de $\mathbb{Z}^n$.

Proposição 2.1.2. *Seja* M *um subgrupo de* $\mathbb{Z}$. *Então existe* $z \in M$ *tal que* $M = \langle z \rangle$.

Demonstração. *Se* $M = \{0\}$, *então, claramente,* $M = \langle 0 \rangle$.

Suponhamos que $M \neq \varnothing$ *e seja* $x \in M \setminus \{0\}$. *Como* M *é um subgrupo de* $\mathbb{Z}$, $-x \in M$. *Assim,* M *tem pelo menos um número inteiro positivo, isto é,* $\{h \in M : h > 0\} \neq \varnothing$. *O conjunto* $\{h \in M : h > 0\}$ *é um subconjunto de* $\mathbb{N}$ *e, como* $\mathbb{N}$ *é um conjunto bem ordenado,* $\{h \in M : h > 0\}$ *tem elemento mínimo. Seja* $z = \min\{h \in M : h > 0\}$. *Mostremos que* $M = \langle z \rangle$. *Por um lado, se* $x \in \langle z \rangle$ *então* $x = tz$, *para algum* $t \in \mathbb{Z}$. *Como* $z \in M$ *e* M *é um subgrupo de* $\mathbb{Z}$, *obtemos* $x \in M$. *Por outro lado, dado* $h \in M$, *uma vez que* $z \neq 0$ *obtemos, pelo algoritmo de Euclides,* $h = q \times z + r$ *para certos* $q, r \in \mathbb{Z}$ *tais que* $0 \leq r < z$. *Então* $r = h - qz$ *é tal que* $0 \leq r < z$. *Dada a definição de* z, *concluímos que* $r = 0$. *Deste modo,* $h = qz$, *isto é,* $h \in \langle z \rangle$.

■

A proposição seguinte, que não vamos demonstrar, estabelece que todo o subgrupo de $\mathbb{Z}^n$ tem uma base e indica o valor máximo do número de elementos dessa base.

Proposição 2.1.3. *Qualquer subgrupo de* $\mathbb{Z}^n$ *admite uma base com, no máximo, n elementos.*

O resultado que se segue é bem conhecido da Álgebra Linear.

Lema 2.1.1. *Consideremos o espaço vetorial* $\mathbb{Q}^n$ *sobre o corpo* $\mathbb{Q}$ *e seja* $A \subseteq \mathbb{Q}^n$. *Então o subespaço vetorial de* $\mathbb{Q}^n$ *gerado por A, que se representa por* $\langle A \rangle_{\mathbb{Q}^n}$, *é constituído por todas as combinações lineares de vetores de A, ou seja:*

$$\langle A \rangle_{\mathbb{Q}^n} = \left\{ \sum_{i=1}^{t} q_i a_i : \ t \in \mathbb{N}, \ a_i \in A, \ q_i \in \mathbb{Q} \right\}.$$

Tendo em atenção este lema, prova-se que:

Proposição 2.1.4. *Seja M um subgrupo de* $\mathbb{Z}^n$. *Então todas as bases de M têm o mesmo número de elementos.*

Demonstração. *Suponhamos que* $B = \{m_1, \ldots, m_r\}$ *e* $B' = \{m_1, \ldots, m_t\}$ *são duas bases de M. Mostremos que* $t \leq r$. *Dado que os elementos de B são linearmente independentes como vetores do espaço vetorial racional* $\mathbb{Q}^n$ *de dimensão n, temos, pela Proposição 2.1.3, que B tem, no máximo, n elementos. O mesmo se verifica para* B'. *Temos, portanto,* $t, \ r \leq n$. *Ora B é uma base do subespaço vetorial V de* $\mathbb{Q}^n$ *gerado por* $\{m_1, \ldots, m_r\}$ *e, como*

$$B' \subseteq M = \langle m_1, \ldots, m_r \rangle_{\mathbb{Z}^n} \subsetneq V = \langle m_1, .., m_r \rangle_{\mathbb{Q}^n},$$

B' *é constituído por vetores (linearmente independentes) de* V. *Uma vez que o espaço vetorial V tem dimensão r, concluímos que* $t \leq r$. *Trocando, neste raciocínio, os papéis de B e* B', *obtemos* $r \leq t$ *e o resultado fica provado.*

■

A proposição que acabámos de provar permite introduzir, sem ambiguidade, a seguinte definição:

Definição 2.1.3. *Para qualquer subgrupo M de* $\mathbb{Z}^n$ *, chama-se* **dimensão** *de M e representa-se por* $\dim M$ *ao número de elementos de uma qualquer base de M.*

Pensando na base canónica de $\mathbb{Z}^n$, obtemos da Definição 2.1.3 que $\dim(\mathbb{Z}^n) = n$. Assim, temos que, para qualquer subgrupo M de $\mathbb{Z}^n$, $\dim M \leq n$.

É importante referir que, relativamente à dimensão de um subgrupo de um grupo, a situação é distinta da situação homóloga para espaços vetoriais. Num espaço vetorial E, de dimensão n,

não é possível haver um subespaço F de E, distinto de E, com dimensão n. Contudo, nos grupos isto é possível. Por exemplo, considerando o grupo $\mathbb{Z}$ de dimensãoo 1, $\{1\}$ é uma base de $\mathbb{Z}$, o subgrupo $2\mathbb{Z}$ de $\mathbb{Z}$ é distinto de $\mathbb{Z}$ e tem também dimensão 1, já que $\{2\}$ é uma base de $2\mathbb{Z}$. Se ampliarmos a base $\{2\}$ com o elemento 3, como 3 não é combinação linear de 2 (uma vez que 2 não divide 3), poder-se-ia pensar que os elementos 2 e 3 de $\mathbb{Z}$ seriam linearmente independentes, o que seria uma contradição porque a dimensão de $\mathbb{Z}$ é 1. No entanto, 2 e 3 não são linearmente independentes, por exemplo, $0 = 3 \times 2 + (-2) \times 3$.

O resultado dos espaços vetoriais que não é válido nos grupos, e que permite que aconteça nos grupos uma situação que, nos espaços vetoriais é impossível, é o seguinte: *dados n vetores de um espaço vetorial, se eles são linearmente dependentes então pelo menos uma deles é combinação linear dos restantes (ou seja, recorrendo ao contra-recíproco, dados n vetores de um espaço vetorial, se nenhum dos vetores é combinação linear dos restantes* $n-1$ *vetores, então os n vetores são linearmente independentes).* A razão pela qual este resultado não é válido no caso dos grupos é que o escalar não nulo, na expressão do vetor nulo como combinação linear dos n vetores, pode não ser invertível (sendo não nulo, ele é invertível num corpo, que é o caso dos espaços vetoriais).

Proposição 2.1.5. *Seja M um subgrupo de* $\mathbb{Z}^n$*, de dimensão k. Então os subgrupos M e* $\mathbb{Z}^k$ *de* $\mathbb{Z}^n$ *são isomorfos.*

Demonstração. *Seja* $B = \{m_1, \ldots, m_k\}$ *uma base de M. Consideremos a aplicação* $f : \mathbb{Z}^k \to M$ *definida por* $f(z_1, \ldots, z_k) = \sum_{i=1}^{k} z_i m_i$*, para quaisquer* $z_1, z_2, \ldots, z_k \in \mathbb{Z}$*. Mostremos que a aplicação* f *é um isomorfismo.*

- f *é injetiva*

  Sejam $(z_1, \ldots, z_k), (z'_1, \ldots, z'_k) \in \mathbb{Z}^k$*. Temos:*

  $$f(z_1, \ldots, z_k) = f(z'_1, \ldots, z'_k) \Rightarrow \sum_{i=1}^{k} z_i m_i = \sum_{i=1}^{k} z'_i m_i \Rightarrow \sum_{i=1}^{k} z_i m_i - \sum_{i=1}^{k} z'_i m_i = 0 \Rightarrow \sum_{i=1}^{k} (z_i - z'_i) m_i = 0.$$

  Como $m_1, \ldots, m_k$ *são linearmente independentes, segue-se que* $z_i - z'_i = 0$*, para qualquer* $i \in \{1, \ldots, k\}$*, ou seja,* $z_i = z'_i$*, para todo* $i \in \{1, \ldots, k\}$*. Logo* $(z_1, \ldots, z_k) = (z'_1, \ldots, z'_k)$ *e, portanto,* f *é injetiva.*

- *f é sobrejetiva*

  Seja $m \in M$. *Então* $m = \sum_{i=1}^{k} z_i m_i$, *para certos* $z_1, z_2, \ldots, z_k \in \mathbb{Z}$, *i.e.,* $m = f(z_1, \ldots, z_k) = m$, *para certo* $(z_1, \ldots, z_k) \in \mathbb{Z}^k$.

- *f é morfismo*

  Sejam $(z_1, \ldots, z_k), \left(z'_1, \ldots, z'_k\right) \in \mathbb{Z}^k$. *Temos:*

$$\begin{aligned} f\left((z_1, \ldots, z_k) + \left(z'_1, \ldots, z'_k\right)\right) &= f\left(z_1 + z'_1, \ldots, z_k + z'_k\right) \\ &= \sum_{i=1}^{k} \left(z_i + z'_i\right) m_i \\ &= \sum_{i=1}^{k} \left(z_i m_i + z'_i mi\right) \\ &= \sum_{i=1}^{k} z_i m_i + \sum_{i=1}^{k} z'_i m_i \\ &= f(z_1, \ldots, z_k) + f\left(z'_1, \ldots, z'_k\right). \end{aligned}$$

■

Corolário 2.1.1. *Dois subgrupos de* $\mathbb{Z}^n$ *são isomorfos se e só se tiverem a mesma dimensão.*

Demonstração. *Sejam* M *e* M' *dois subgrupos de* $\mathbb{Z}^n$. *Suponhamos que* M *e* M' *são isomorfos e sejam* $k = \dim M$ *e* $t = \dim M'$. *Pela Proposição 2.1.5,* M *é isomorfo a* $\mathbb{Z}^k$ *e* M' *é isomorfo a* $\mathbb{Z}^t$. *Como* M *e* M' *são isomorfos obtemos, dada a transitividade da relação de isomorfismo,* $\mathbb{Z}^k$ *isomorfo a* $\mathbb{Z}^t$. *Seja* $\phi : \mathbb{Z}^k \to \mathbb{Z}^t$ *um isomorfismo. Cálculos simples mostram que, considerando a base canónica de* $\mathbb{Z}^k$, $\{e_1, \ldots, e_k\}$, *o conjunto* $\{\phi(e_1), \ldots, \phi(e_k)\}$ *é uma base de* $\mathbb{Z}^t$. *Assim* $\dim \mathbb{Z}^t = k$, *pelo que* $t = k$.

Reciprocamente, suponhamos que $\dim M = \dim M' = k$. *De novo a Proposição 2.1.5 garante que* M *é isomorfo a* $\mathbb{Z}^k$. *Do mesmo modo,* M' *é isomorfo a* $\mathbb{Z}^k$. *Como a relação de isomorfismo é simétrica e transitiva, concluímos que* M *e* M' *são isomorfos.*

■

2.2 Matrizes com entradas inteiras e fatores invariantes de um subgrupo de $\mathbb{Z}^n$

Nesta secção vamos estudar as matrizes com entradas inteiras, dado que, como iremos verificar, os resultados obtidos para estas matrizes podem ser de algum modo ”traduzidos”para subgrupos de $\mathbb{Z}^n$.

Definição 2.2.1. *Sejam n e* $1 \leq i, j \leq n$ $(i \neq j)$ *números inteiros positivos. As seguintes operações efetuadas sobre as linhas (colunas) de uma matriz A designam-se por* **operações elementares sobre linhas** *(operações elementares sobre colunas):*

- E_1 : *substituição de uma linha (coluna) da matriz A pelo seu produto por* -1*;*
- E_2 : *substituição de uma linha (coluna) de A pela sua soma com qualquer outra linha (coluna) multiplicada por um número inteiro qualquer;*
- E_3 : *troca de duas linhas (colunas) quaisquer.*

Definição 2.2.2. *Sejam n e* $1 \leq i, j \leq n$ $(i \neq j)$ *números inteiros positivos.*

Chamam-se **matrizes linha-elementares de ordem** *n e representam-se como se indica de seguida, às matrizes assim definidas:*

- $L_{i \leftrightarrow j}$: *é a matriz obtida a partir da matriz identidade* I_n *trocando a linha i com a linha* j*;*
- $L_{i \leftarrow -i}$: *é a matriz obtida a partir de* I_n *substituindo a linha i pelo seu produto por* -1*;*
- $L_{j \leftarrow j+zi}$: *é a matriz que se obtém de* I_n *substituindo a linha* j *pela sua soma com a linha i multiplicada por qualquer* $z \in Z$.

De modo análogo definem-se **matrizes coluna-elementares**. Estas matrizes representam-se, respetivamente, por: $C_{i \leftrightarrow j}$, $C_{i \leftarrow -i}$ e $C_{j \leftarrow j+zi}$.

Observemos que a matriz identidade I_n é, simultaneamente, matriz linha-elementar e matriz coluna-elementar.

Cálculos de rotina permitem demonstrar a proposição seguinte:

Proposição 2.2.1. *Sejam* i, j *dois números inteiros positivos,* $z \in \mathbb{Z}$ *e* A *uma matriz quadrada de ordem n sobre* $\mathbb{Z}$*. Então:*

i) $\det\left(L_{i\leftrightarrow j}\right) = \det\left(C_{i\leftrightarrow j}\right) = -1$*;*

ii) $L_{i\leftrightarrow j}^{-1} = L_{j\leftrightarrow i}$ *e* $C_{i\leftrightarrow j}^{-1} = C_{j\leftrightarrow i}$*;*

iii) $\det\left(L_{i\leftarrow -i}\right) = \det\left(C_{i\leftarrow -i}\right) = -1$*;*

iv) $L_{i\leftarrow -i}^{-1} = L_{i\leftarrow -i}$ *e* $C_{i\leftarrow -i}^{-1} = C_{i\leftarrow -i}$*;*

v) $\det\left(L_{j\leftarrow j+zi}\right) = \det\left(C_{j\leftarrow j+zi}\right) = 1$*;*

vi) $L_{j\leftarrow j+zi}^{-1} = L_{j\leftarrow j-zi}$ *e* $C_{j\leftarrow j+zi}^{-1} = C_{j\leftarrow j-zi}$*;*

vii) *A matriz* $L_{i\leftrightarrow j}A$ *é a matriz obtida a partir da matriz A trocando a linha i de A com a linha j de A;*

A matriz $AC_{i\leftrightarrow j}$ *é a matriz resultante da troca da colunas i de A com a coluna j de A;*

viii) *A matriz* $L_{i\leftarrow -i}A$ *é a matriz obtida a partir da matriz A, substituindo a linha i de A pelo seu produto por* -1*;*

A matriz $AC_{i\leftarrow -i}$ *é a matriz que resulta de A substituindo a coluna i de A pelo seu produto por* -1*;*

ix) *A matriz* $L_{j\leftarrow j+zi}A$ *é a matriz obtida a partir da matriz A, substituindo a linha j de A pela sua soma com a linha i multiplicada por z* $(z \in \mathbb{Z})$*;*

A matriz $AC_{j\leftarrow j+zi}$ *é a matriz resultante de A substituindo a coluna j de A pela sua soma com a coluna i multiplicada por z* $(z \in \mathbb{Z})$.

De notar que as alíneas ii), iv) e vi) afirmam que as matrizes linha-elementares e coluna-elementares são matrizes invertíveis. Prova-se que o produto de matrizes elementares é uma matriz invertível.

Definição 2.2.3. *Sejam A e B duas matrizes com entradas inteiras.*

Diz-se que a matriz A é **equivalente** *à matriz B e escreve-se* $A \sim B$*, se existe uma matriz linha-elementar P e uma matriz coluna-elementar Q tal que* $A = PBQ$.

Com base em ii), iv) e vi) da Proposição 2.2.1, verifica-se que " $\sim$ " é uma relação de equivalência.

Proposição 2.2.2. *Sejam A e B duas matrizes quaisquer com entradas inteiras.*

A relação binária definida em 2.2.3 é uma relação de equivalência.

Em virtude da Proposição 2.2.2, sempre que $A \sim B$, afirmaremos, sem ambiguidade, que as **matrizes** A e B são **equivalentes**.

Quando multiplicamos uma matriz qualquer por uma matriz linha-elementar (coluna-elementar), dizemos que estamos a efetuar operações elementares sobre as linhas (colunas) da matriz dada. A principal diferença entre trabalhar com uma matriz com entradas inteiras e trabalhar com uma matriz com entradas num corpo K, prende-se com o facto de que, para além das matrizes $L_{i\leftrightarrow j}$, $L_{i\leftarrow -i}$, $L_{j\leftarrow j+zi}$, $C_{i\leftrightarrow j}$, $C_{i\leftarrow -i}$ e $C_{j\leftarrow j+zi}$, as matrizes da forma $L_{i\leftarrow qi}$ e $C_{i\leftarrow qi}$ com entradas em K, com $q \in K\setminus\{0\}$, igualmente chamadas matrizes elementares, são também invertíveis. Portanto, a condução do processo de eliminação de Gauss-Jordan numa matriz com entradas num corpo K permite levar essa matriz a uma matriz da forma $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ que é, como sabemos, equivalente à matriz inicial. Como veremos mais adiante, qualquer matriz com entradas inteiras é equivalente a uma matriz da forma $\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$, onde D é uma matriz diagonal. Por $\mathbb{Z}$ não ser corpo, o procedimento de "transformação" da matriz inicial numa matriz da forma referida não é tão simples.

Proposição 2.2.3. *Seja A uma matriz, do tipo* $s \times t$*, com entradas inteiras. Então a matriz A é equivalente a uma matriz da forma*

$$\begin{bmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & d_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix}$$

onde $r \leq \min\{s,t\}$, $\{d_1,\dots,d_r\} \subset \mathbb{N}$ *e* d_i *divide* d_{i+1} *para todo o* $i \in \{1,2,\dots r-1\}$.

A demonstração desta proposição é construtiva no sentido em que consiste na apresentação de um método que permite levar a matriz dada a uma matriz da forma indicada. Por esta razão vamos apresentar alguns exemplos que ilustram, em todas as situações possíveis, o processo a seguir na obtenção de uma matriz da forma indicada.

Exemplo 2.2.1

Seja $A = \begin{bmatrix} -3 & 1 & 4 \\ 1 & 5 & -2 \end{bmatrix}$.

O nosso objetivo é mostrar que a matriz A é equivalente a uma matriz da forma apresentada na Proposição 2.2.3, isto é, que existem matrizes invertíveis P e Q tais que:

$$PAQ = \begin{bmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \end{bmatrix},$$

onde d_1 divide d_2.

Como a matriz A é do tipo 2×3, começamos por considerar as matrizes I_2 e I_3 que colocamos, respetivamente, à esquerda e à direita da matriz A, como se segue:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -3 & 1 & 4 \\ 1 & 5 & -2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Com o objetivo de transformar a matriz A numa matriz da forma $\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$, faremos operações elementares sobre as linhas e sobre as colunas de A de tal forma que as operações efetuadas nas linhas da matriz A são também efetuadas (e apenas) na matriz I_2 e as operações realizadas nas colunas da matriz A são também efetuadas (e apenas) na matriz I_3. Quando atingirmos a forma pretendida para a matriz A, as matrizes que surgirem à esquerda e à direita dessa matriz serão, respetivamente, as matrizes P e Q que procuramos. O primeiro passo do procedimento é colocar, sempre que possível, na posição $(1,1)$ da matriz A, o menor elemento da matriz, em valor absoluto.

Vamos acompanhando o processo indicando as operações elementares efetuadas.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -3 & 1 & 4 \\ 1 & 5 & -2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \xrightarrow{L_{1\leftrightarrow 2}A} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 5 & -2 \\ -3 & 1 & 4 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Neste exemplo, como a entrada que ocupa a posição $(1,1)$ da matriz A divide todos os elementos da linha 1 e todos os elementos da coluna 1, usando operações elementares do tipo E_1 continuamos o processo anulando todas as restantes entradas da linha 1 e da coluna 1:

$$\xrightarrow{AC_{2\leftarrow 2+(-5).1}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & -2 \\ -3 & 16 & 4 \end{bmatrix} \begin{bmatrix} 1 & -5 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{AC_{3\leftarrow 3+2.1}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -3 & 16 & -2 \end{bmatrix} \begin{bmatrix} 1 & -5 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{L_{2\leftarrow 2+3.1A}} \begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 16 & -2 \end{bmatrix} \begin{bmatrix} 1 & -5 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Repetimos o processo para a entrada $(2,2)$:

$$\xrightarrow{AC_{2\leftrightarrow 3}} \begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & 16 \end{bmatrix} \begin{bmatrix} 1 & 2 & -5 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

De novo, como $-2 \mid 16$, anulamos a entrada $(2,3)$ recorrendo a uma operação elementar do tipo E_1:

$$\xrightarrow{AC_{2\leftarrow -2}} \begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 16 \end{bmatrix} \begin{bmatrix} 1 & -2 & -5 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}$$

$$\xrightarrow{AC_{3\leftarrow 3+(-8).2}} \begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} \begin{bmatrix} 1 & -2 & 11 \\ 0 & 0 & 1 \\ 0 & -1 & 8 \end{bmatrix}.$$

Se a entrada $(2,2)$ não dividisse uma das entradas da linha 2 ou coluna 2, o processo seria um

pouco mais complexo – este processo está ilustrado no próximo exemplo.

A matriz A foi, assim, *transformada* na matriz $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$, que tem a forma pretendida. As matrizes P e Q procuradas são, respetivamente, $P = \begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix}$ e $Q = \begin{bmatrix} 1 & -2 & 11 \\ 0 & 0 & 1 \\ 0 & -1 & 8 \end{bmatrix}$. De facto, por um lado P e Q são matrizes invertíveis por serem produto, respetivamente, de matrizes linha-elementares e coluna-elementares e, por outro lado ,

$$\begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix} \cdot \begin{bmatrix} -3 & 1 & 4 \\ 1 & 5 & -2 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & 11 \\ 0 & 0 & 1 \\ 0 & 1 & 8 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}.$$

Exemplo 2.2.2

Consideremos agora a matriz $A = \begin{bmatrix} 4 & 6 & 8 \\ 5 & 10 & -12 \end{bmatrix}$. Temos:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 4 & 6 & 8 \\ 5 & 10 & -12 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

O menor elemento da matriz A, em valor absoluto, já ocupa a posição $(1,1)$. Acontece que o número que ocupa essa posição não divide, todos os elementos da linha 1 (4 não divide 6) e, assim, o processo não é tão simples como no exemplo anterior. Usando o algoritmo da divisão inteira, temos que $6 = 4 \cdot 1 + 2$. Como 2 divide 4, efetuamos na matriz A a operação elementar $AC_{2 \leftarrow 2+(-1)\cdot 1}$, seguida da operação $AC_{1 \leftrightarrow 2}$, obtendo uma matriz equivalente que tem na posição $(1,1)$ um número que divide todas as entradas da linha 1 :

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 4 & 2 & 8 \\ 5 & 5 & -12 \end{bmatrix} \quad \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{AC_{1 \leftrightarrow 2}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 2 & 4 & 8 \\ 5 & 5 & -12 \end{bmatrix} \quad \begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

É claro que o resto da divisão inteira de a_{11} por a_{12} pode não dividir a_{11} . No entanto, o algoritmo

de Euclides garante que ao fim de um número finito de divisões se obtém r tal que r divide a_{11}. Procedendo de modo análogo para as entradas da primeira coluna, observamos que 5 não divide 2**.** Como $5 = 2 \cdot 2 + 1$**,** fazemos

$$\xrightarrow[L_{2\leftarrow 2+(-2)\cdot 1}]{} \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 4 & 8 \\ 1 & -3 & -28 \end{bmatrix} \begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow[L_{1\leftrightarrow 2}]{} \begin{bmatrix} -2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -3 & -28 \\ 2 & 4 & 8 \end{bmatrix} \begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Estamos agora numa situação em tudo análoga à do Exemplo 2.2.1, pelo que procedemos como então indicámos:

$$\xrightarrow[AC_{2\leftarrow 2+3\cdot 1}]{} \begin{bmatrix} -2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & -28 \\ 2 & 10 & 8 \end{bmatrix} \begin{bmatrix} -1 & -2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow[AC_{3\leftarrow 3+28\cdot 1}]{} \begin{bmatrix} -2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 2 & 10 & 64 \end{bmatrix} \begin{bmatrix} -1 & -2 & -28 \\ 1 & 3 & 28 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow[L_{2\leftarrow 2+(-2)\cdot 1}]{} \begin{bmatrix} -2 & 1 \\ 5 & -2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 10 & 64 \end{bmatrix} \begin{bmatrix} -1 & -2 & -28 \\ 1 & 3 & 28 \\ 0 & 0 & 1 \end{bmatrix}.$$

O processo continua agora com a análise da entrada $(2,2)$. Ora $64 = 10 \cdot 6 + 4$,

$$\xrightarrow[AC_{3\leftarrow 3+(-6)\cdot 2}]{} \begin{bmatrix} -2 & 1 \\ 5 & -2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 10 & 4 \end{bmatrix} \begin{bmatrix} -1 & -2 & -16 \\ 1 & 3 & 10 \\ 0 & 0 & 1 \end{bmatrix}.$$

Como $10 = 4 \cdot 2 + 2$,

$$\xrightarrow[AC_{2\leftarrow 2+(-2)\cdot 3}]{} \begin{bmatrix} -2 & 1 \\ 5 & -2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \end{bmatrix} \begin{bmatrix} -1 & 30 & -16 \\ 1 & -17 & 10 \\ 0 & -2 & 1 \end{bmatrix}$$

$$\xrightarrow[AC_{3\leftarrow 3+(-2)\cdot 2}]{} \begin{bmatrix} -2 & 1 \\ 5 & -2 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} \quad \begin{bmatrix} -1 & 30 & -76 \\ 1 & -17 & 44 \\ 0 & -2 & 5 \end{bmatrix}.$$

Finalmente,

$$\begin{bmatrix} -2 & 1 \\ 5 & -2 \end{bmatrix} \cdot \begin{bmatrix} 4 & 6 & 8 \\ 5 & 10 & -12 \end{bmatrix} \cdot \begin{bmatrix} -1 & 30 & -76 \\ 1 & -17 & 44 \\ 0 & -2 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}.$$

Assim, a matriz inicial $A = \begin{bmatrix} 4 & 6 & 8 \\ 5 & 10 & -12 \end{bmatrix}$ é equivalente à matriz $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$.

Aos elementos $d_1, \ldots, d_r$ referidos na Proposição 2.2.3, damos o nome de **fatores invariantes** da matriz A. Quer no Exemplo 2.2.1, quer no Exemplo 2.2.2, os fatores invariantes da matriz A são 1 e 2.

Mostramos de seguida que, para cada matriz $A \in M_{s\times t}(\mathbb{Z})$, os fatores invariantes estão univocamente determinados. Para tal, definimos ***menor de ordem*** k ***de*** A $(k \leq \min\{s,t\})$ como sendo o determinante de qualquer submatriz quadrada de A de ordem k. Para cada $k \leq \min\{s,t\}$, representamos por $D_k(A)$ o máximo divisor comum de todos os menores de ordem k de A. Cálculos simples mostram que $D_k(A)$ não se altera quando se efetua na matriz A qualquer uma das operações elementares sobre linhas ou colunas.

Proposição 2.2.4. *Seja* $A \in M_{s\times t}(\mathbb{Z})$. *Então:*

i) $D_k\left(L_{i\leftrightarrow j}A\right) = D_k(A) = D_k(AC_{i\leftrightarrow j})$;

ii) $D_k(L_{i\leftarrow -i}A) = D_k(A) = D_k(AC_{i\leftarrow -i})$;

iii) $D_k\left(L_{j\leftarrow j+zi}A\right) = D_k(A) = D_k\left(AC_{j\leftarrow j+zi}\right)$.

■

Corolário 2.2.1. *Para quaisquer matrizes equivalentes A e B,* $D_k(A) = D_k(B)$, *para qualquer* $k \leq \min\{s,t\}$.

Proposição 2.2.5. *Duas matrizes com entradas inteiras são equivalentes se e só se têm os mesmos fatores invariantes.*

Demonstração. *Sejam A e B matrizes com entradas inteiras e sejam*

$$A_1 = \begin{bmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & d_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix} \text{ e } B_1 = \begin{bmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & d_s & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix}$$

as matrizes equivalentes, respetivamente, a A e a B, a que se refere a Proposição 2.2.3. Como $\sim$ *é uma relação de equivalência , basta provar que* $A_1 \sim B_1$ *se e só se* $r = s$ *e* $d_i = d_i'$ *, para todo* $1 \leq i \leq r$ *. Por um lado, é claro que se* $r = s$ *e* $d_i = d_i'$ *para todo o i, então* $A_1 \sim B_1$.

Reciprocamente, se $A_1 \sim B_1$*, então pelo Corolário 2.2.1,* $d_1 \times \dots \times d_k = D_k(A_1) = D_k(B_1) = d_1' \times \dots \times d_k'$*, para qualquer* $1 \leq k \leq r = s$.

■

Os resultados obtidos para matrizes podem ser ”traduzidos” para subgrupos de $\mathbb{Z}^n$. Começamos com uma proposição que permite obter bases novas de um subgrupo M de $\mathbb{Z}^n$, a partir de uma qualquer base de M.

Proposição 2.2.6. *Sejam M um subgrupo de* $\mathbb{Z}^n$ *e* $\{m_1, \dots, m_i, \dots, m_j, \dots, m_r\}$ *uma base de M.*

Então:

i) $\{m_1, \dots, m_j, \dots, m_i, \dots, m_r\}$ *é uma base de M;*

ii) $\{m_1, \dots, -m_i, \dots, m_j, \dots, m_r\}$ *é uma base de M;*

iii) $\{m_1, \dots, m_j + zm_i, \dots, m_r\}$ *é uma base de M, para qualquer* $z \in \mathbb{Z}$.

Demonstração. *Como* $M = \langle m_1, m_2 \dots, m_r \rangle$*, os elementos de cada um dos conjuntos indicados em i), ii) e iii) são combinação linear de* $m_1, m_2, \dots, m_r$ *através de coordenadas inteiras univocamente determinadas. Considerando a matriz cujas colunas são estas coordenadas, a Proposição*

2.2.1 garante que os elementos de cada um dos referidos conjuntos são linearmente independentes. Em cada um dos casos, estes elementos são claramente geradores de M e, deste modo, constituem uma base de M.

■

As mudanças de base apresentadas na proposição anterior, designam-se por **mudanças elementares de base**.

Proposição 2.2.7. *Seja* $B = \begin{bmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{nn} \end{bmatrix}$ *uma matriz com entradas inteiras e, para cada* $1 \le i \le n$, *seja* $b_i = (b_{i1}, \dots b_{in}) \in \mathbb{Z}^n$ *a linha i de B.*

Então o conjunto $\{b_1, \dots, b_n\}$ *é uma base de* $\mathbb{Z}^n$ *se e só se* $\det B \in \{-1, 1\}$.

Demonstração. *Suponhamos que* $\{b_1, \dots, b_n\}$ *é uma base de* $\mathbb{Z}^n$. *Então* $\mathbb{Z}^n = \langle b_1, b_2, .., b_n \rangle$ *e, portanto, em particular, cada elemento* e_i *da base canónica de* $\mathbb{Z}^n$ *é tal que* $e_i = \sum_{j=1}^{n} z_{ij} b_j$, *ou seja,*

$$\begin{bmatrix} z_{11} & \dots & z_{1n} \\ \dots & \dots & \dots \\ z_{n1} & \dots & z_{nn} \end{bmatrix} . \begin{bmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{nn} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix} .$$

Uma vez que $\det I_n = 1$ *e que o determinante do produto de matrizes é igual ao produto dos determinantes de cada uma das matrizes, temos que* $\det B \in \{-1, 1\}$.

Reciprocamente, suponhamos que $\det B \in \{-1, 1\}$. *Então* $\det B \neq 0$ *e, portanto, a matriz B é invertível. Deste modo, o sistema de equações* $(x_1, \dots, x_n) \cdot B = z$ *tem uma única solução,* $z \cdot B^{-1}$, *qualquer que seja* $z \in \mathbb{Z}^n$. *Isto é o mesmo que dizer que qualquer elemento de* $\mathbb{Z}^n$ *se escreve de modo único como combinação linear dos elementos* $b_1, b_2, \dots, b_n$ *de* $\mathbb{Z}^n$. *Como* $\dim \mathbb{Z}^n = n$ *segue-se que* $\{b_1, \dots, b_n\}$ *é uma base de* $\mathbb{Z}^n$.

■

Proposição 2.2.8. *Seja M um subgrupo de* $\mathbb{Z}^n$ *de dimensão r. Então existe uma base* $\{f_1, \dots, f_r, \dots, f_n\}$ *de* $\mathbb{Z}^n$ *e* $\{d_1, \dots, d_r\} \subsetneq \mathbb{N}$ *tais que* d_i *divide* d_{i+1} *para todo o i, e* $\{d_1 f_1, \dots, d_r f_r\}$ *é uma base de M.*

Demonstração. *Seja* $\{m_1,...,m_r\}$ *uma base de M onde* $m_i = (m_{i1},...,m_{in})$ *para todo o* $1 \le i \le r$. *A Proposição 2.2.3 garante a existência de matrizes P e Q tais que:*

$$P\begin{bmatrix} m_{11} & \dots & m_{1n} \\ \dots & \dots & \dots \\ m_{r1} & \dots & m_{rn} \end{bmatrix} Q = \begin{bmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & d_s & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix},$$

para algum $0 \le s \le \min\{r,n\}$, $\{d_1,...,d_s\} \subsetneq \mathbb{N}$ *e* d_i *divide* d_{i+1} *para todo o* $1 \le i \le s-1$. *Como as matrizes P e Q, sendo produto de matrizes elementares, são invertíveis, a característica da matriz* $\begin{bmatrix} m_{11} & \dots & m_{1n} \\ \dots & \dots & \dots \\ m_{r1} & \dots & m_{rn} \end{bmatrix}$, *que é r, dado que* $\{m_1,...,m_r\}$ *é base, e a característica da matriz*

$$\begin{bmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & d_s & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix}$$

são iguais e, consequentemente, r = s.

Considerando

$$\begin{bmatrix} c_{11} & \dots & c_{1n} \\ \dots & \dots & \dots \\ c_{r1} & \dots & c_{rn} \end{bmatrix} = P\begin{bmatrix} m_{11} & \dots & m_{1n} \\ \dots & \dots & \dots \\ m_{r1} & \dots & m_{rn} \end{bmatrix},$$

e $c_i = (c_{i1},...c_{in})$ *para todo o i, temos que* $\{c_1,...,c_r\}$ *é uma base de M, pois é o resultado da realização de um número finito de mudanças elementares de base efetuadas na base* $\{m_1,...,m_r\}$.

Finalmente, determinando a inversa da matriz Q e representando-a por $Q^{-1} = [f_{ij}]$ *temos que* $\det Q^{-1} \in \{-1,1\}$ *dado a matriz Q ser produto de matrizes coluna-elementares, e o determinante destas matrizes ser* ± 1 *(Proposição 2.2.1)* .

Então, como $\det Q^{-1} \in \{-1, 1\}$*, concluimos, usando a Proposição 2.2.7, que* $\{f_1, \ldots, f_n\}$ *, com* $f_i = (f_{i1}, \ldots f_{in})$*, é uma base de* $\mathbb{Z}^n$*. Como*

$$\begin{bmatrix} c_{11} & \ldots & c_{1n} \\ \ldots & \ldots & \ldots \\ c_{r1} & \ldots & c_{rn} \end{bmatrix} = \begin{bmatrix} d_1 & 0 & 0 & \ldots & \ldots & 0 \\ 0 & d_2 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & 0 & d_r & 0 & \ldots & 0 \end{bmatrix} \begin{bmatrix} f_{11} & \ldots & f_{1n} \\ \ldots & \ldots & \ldots \\ f_{n1} & \ldots & f_{nn} \end{bmatrix},$$

obtemos $c_i = d_i f_i$ *para todo o* $i \in \{1, \ldots, n\}$ *e, portanto, dado que* $\{c_1, c_2, \ldots, c_r\}$ *é uma base de M, temos que* $\{d_1 f_1, \ldots, d_r f_r\}$ *é uma base de M.*

■

Definição 2.2.4. *Seja M um subgrupo de* $\mathbb{Z}^n$*. Dada uma base qualquer de M dá-se o nome de* **fatores invariantes do subgrupo** *M aos fatores invariantes da matriz cujas linhas são as coordenadas de cada um dos elementos da base de M.*

Sejam M um subgrupo de $\mathbb{Z}^n$ de dimensão r, $\{f_1, \ldots, f_r, \ldots, f_n\}$ uma base de $\mathbb{Z}^n$ e $\{d_1 f_1, \ldots, d_r f_r\}$ uma base de M com $\{d_1, \ldots, d_r\} \subsetneq \mathbb{N}$ tais que d_i divide d_{i+1} para todo o i. Então um elemento $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ pertence a M se e só se as suas coordenadas $(z_1, \ldots, z_n)$ relativamente à base $\{f_1, \ldots, f_r, \ldots, f_n\}$ satisfazem:

$$\begin{aligned} z_1 &\equiv 0 \,(\mathrm{mod}\, d_1) \\ z_2 &\equiv 0 \,(\mathrm{mod}\, d_2) \\ &\ldots \\ z_r &\equiv 0 \,(\mathrm{mod}\, d_r) \\ z_{r+1} &= 0. \\ &\ldots \\ z_n &= 0. \end{aligned}$$

Como $(z_1,\ldots,z_n)$ são as coordenadas de x relativamente à base $\{f_1,\ldots,f_n\}$,

$$x = (x_1,\ldots,x_n) = z_1 f_1 + \ldots + z_n f_n$$

e, portanto, considerando $f_i = (f_{i1},\ldots f_{in})$ para todo o i, temos que:

$$[x_1\ldots x_n] = [z_1\ldots z_n]\cdot \begin{bmatrix} f_{11} & \cdots & f_{1n} \\ \ldots & \ldots & \ldots \\ f_{n1} & \cdots & f_{nn} \end{bmatrix},$$

o que implica :

$$[z_1\ldots z_n] = [x_1\ldots x_n]\cdot \begin{bmatrix} g_{11} & \cdots & g_{1n} \\ \ldots & \ldots & \ldots \\ g_{n1} & \cdots & g_{nn} \end{bmatrix} \quad ,$$

onde a matriz com as entradas g_{ij} é a inversa da matriz com entradas f_{ij} (a matriz Q na demonstração da Proposição 2.2.8). Assim, o elemento $x = (x_1,\ldots x_n) \in \mathbb{Z}^n$ pertence a M se e só se:

$$\begin{aligned} &g_{11}x_1 + \ldots + g_{n1}x_n \equiv 0 \,(\bmod d_1) \\ &g_{12}x_1 + \ldots + g_{2n}x_n \equiv 0 \,(\bmod d_2) \\ &\ldots \\ &g_{1r}x_1 + \ldots + g_{nr}x_n \equiv 0 \,(\bmod d_r) \\ \\ &g_{1(r+1)}x_1 + \ldots + g_{n(r+1)}x_n = 0 \\ &\ldots \\ &g_{1n}x_1 + \ldots\ldots\ldots + g_{nn}x_n = 0. \end{aligned}$$

Estas ”equações” designam-se, geralmente, por equações de M relativamente à base $\{e_1,\ldots,e_n\}$ ou, simplesmente, por **equações de** M.

Se algum $d_i = 1$, a equação correspondente pode ser eliminada pois é uma redundância.

Exemplo 2.2.3

Seja $M = \langle m_1, m_2, m_3\rangle$, com $m_1 = (3,2,-1)$, $m_2 = (4,-1,5)$ e $m_3 = (2,-1,7)$, um subgrupo de $\mathbb{Z}^3$.

Determinemos então as equações de M. Comecemos por determinar os fatores invariantes de M. Recordemos que os fatores invariantes de M são os fatores invariantes da matriz cujas linhas são ocupadas pelas coordenadas dos elementos da base de M.

Temos:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 3 & -2 & 1 \\ 4 & -1 & 5 \\ 2 & -1 & 7 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{AC_{1\leftrightarrow 3}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & -2 & 3 \\ 5 & -1 & 4 \\ 7 & -1 & 2 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$$\xrightarrow{AC_{2\leftarrow 2+2\cdot 1}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 3 \\ 5 & 9 & 4 \\ 7 & 13 & 2 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 2 & 0 \end{bmatrix}$$

$$\xrightarrow{AC_{3\leftarrow 3+(-3)\cdot 1}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 5 & 9 & -11 \\ 7 & 13 & -19 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 2 & -3 \end{bmatrix}$$

$$\xrightarrow{L_{2\leftarrow 2+(-5)\cdot 1}A} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 9 & -11 \\ 7 & 13 & -19 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 2 & -3 \end{bmatrix}$$

$$\xrightarrow{L_{3\leftarrow 3+(-7)\cdot 1}A} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ -7 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 9 & -11 \\ 0 & 13 & -19 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 2 & -3 \end{bmatrix}$$

$$\xrightarrow{AC_{3\leftarrow -3}} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ -7 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 9 & 11 \\ 0 & 13 & 19 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 2 & 3 \end{bmatrix}$$

$$\xrightarrow{AC_{2\leftarrow 2+(-1)\cdot 3}} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ -7 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & 11 \\ 0 & -6 & 19 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & -1 \\ 0 & 1 & 0 \\ 1 & -1 & 3 \end{bmatrix}$$

$$\xrightarrow{AC_{2\leftarrow -2}} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ -7 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 11 \\ 0 & 6 & 19 \end{bmatrix} \quad \begin{bmatrix} 0 & -1 & -1 \\ 0 & -1 & 0 \\ 1 & 1 & 3 \end{bmatrix}$$

$$\xrightarrow{L_{3\leftarrow 3+(-3)\cdot 2}A} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 8 & -3 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 11 \\ 0 & 0 & -14 \end{bmatrix} \quad \begin{bmatrix} 0 & -1 & -1 \\ 0 & -1 & 0 \\ 1 & 1 & 3 \end{bmatrix}$$

$$\xrightarrow[AC_{3\leftarrow 3+(-5)\cdot 2}]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 8 & -3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & -14 \end{bmatrix} \begin{bmatrix} 0 & -1 & 4 \\ 0 & -1 & 5 \\ 1 & 1 & -2 \end{bmatrix}$$

$$\xrightarrow[L_{3\leftarrow 3+14\cdot 2A}]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ -62 & 11 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 28 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 & 4 \\ 0 & -1 & 5 \\ 1 & 1 & -2 \end{bmatrix}$$

$$\xrightarrow[AC_{2\leftrightarrow 3}]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ -62 & 11 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 28 \end{bmatrix} \begin{bmatrix} 0 & 4 & -1 \\ 0 & 5 & -1 \\ 1 & -2 & 1 \end{bmatrix}$$

$$\xrightarrow[AC_{3\leftarrow 3+(-2)\cdot 2}]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ -62 & 11 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 28 \end{bmatrix} \begin{bmatrix} 0 & 4 & -9 \\ 0 & 5 & -11 \\ 1 & -2 & 5 \end{bmatrix}$$

Finalmente,

$$\begin{bmatrix} -1 & 0 & 0 \\ -5 & 1 & 0 \\ -62 & 11 & 1 \end{bmatrix} \cdot \begin{bmatrix} 3 & -2 & 1 \\ 4 & -1 & 5 \\ 2 & -1 & 7 \end{bmatrix} \cdot \begin{bmatrix} 0 & 4 & -9 \\ 0 & 5 & -11 \\ 1 & -2 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 28 \end{bmatrix}$$

e, portanto, os fatores invariantes de M são 1 e 28 e as equações de M são:

$$\begin{aligned} x_3 &\equiv 0 \pmod 1 \\ 4x_1 + 5x_2 - 2x_3 &\equiv 0 \pmod 1 \\ -9x_1 - 11x_2 + 5x_3 &\equiv 0 \pmod{28}. \end{aligned}$$

Como as duas primeiras equações são triviais, concluimos que:

$(x_1, x_2, x_3) \in M$ se e só se $-9x_1 - 11x_2 + 5x_3$ é um múltiplo de 28.

Definição 2.2.5. *Um subgrupo M de* $\mathbb{Z}^n$ *diz-se um* **subgrupo homogéneo** *se, na lista das equações de M, não constar qualquer congruência, o que equivale a dizer que os fatores invariantes de M são todos iguais a* 1.

Exemplo 2.2.4

Seja $M = \langle m_1, m_2, m_3 \rangle$ com $m_1 = (3,-2,1,0)$, $m_2 = (4,-1,5,1)$ e $m_3 = (2,-1,7,2)$, um subgrupo de $\mathbb{Z}^4$. Determinemos então as equações de M. Comecemos por determinar os fatores invariantes de M. Tal como anteriormente, temos:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 3 & -2 & 1 & 0 \\ 4 & -1 & 5 & 1 \\ 2 & -1 & 7 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{AC_{1\leftrightarrow 3}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & -2 & 3 & 0 \\ 5 & -1 & 4 & 1 \\ 7 & -1 & 2 & 2 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{AC_{2\leftarrow 2+2\cdot 1}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 3 & 0 \\ 5 & 9 & 4 & 1 \\ 7 & 13 & 2 & 2 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{AC_{3\leftarrow 3+(-3)\cdot 1}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 9 & -11 & 1 \\ 7 & 13 & -19 & 2 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 2 & -3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{L_{2\leftarrow 2+(-5)\cdot 1}A} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 9 & -11 & 1 \\ 7 & 13 & -19 & 2 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 2 & -3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{L_{3\leftarrow 3+(-7)\cdot 1}A} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ -7 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 9 & -11 & 1 \\ 0 & 13 & -19 & 2 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 2 & -3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow[AC_{2\leftrightarrow 4}]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ -7 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -11 & 9 \\ 0 & 2 & -19 & 13 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & -3 & 2 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$\xrightarrow[L_{3\leftarrow 3+(-3)\cdot 2}A]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 3 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -11 & 9 \\ 0 & 0 & 3 & -5 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & -3 & 2 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$\xrightarrow[AC_{3\leftarrow 3+11\cdot 2}]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 3 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 3 & -5 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & -3 & 2 \\ 0 & 1 & 11 & 0 \end{bmatrix}$$

$$\xrightarrow[AC_{4\leftarrow 4+(-9)\cdot 2}]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 3 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & -5 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & -3 & 2 \\ 0 & 1 & 11 & -9 \end{bmatrix}$$

$$\xrightarrow[AC_{4\leftarrow 4+2\cdot 3}]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 3 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & -3 & -4 \\ 0 & 1 & 11 & 13 \end{bmatrix}$$

$$\xrightarrow[AC_{3\leftrightarrow 4}]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 3 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 \end{bmatrix} \begin{bmatrix} 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & -4 & -3 \\ 0 & 1 & 13 & 11 \end{bmatrix}$$

$$\xrightarrow[AC_{4\leftarrow 4+(-3)\cdot 3}]{} \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 3 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 2 & -5 \\ 0 & 0 & 1 & -3 \\ 1 & 0 & -4 & 9 \\ 0 & 1 & 13 & -28 \end{bmatrix}$$

Finalmente,

$$\begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 3 & -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 3 & -2 & 1 & 0 \\ 4 & -1 & 5 & 1 \\ 2 & -1 & 7 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 2 & -5 \\ 0 & 0 & 1 & -3 \\ 1 & 0 & -4 & 9 \\ 0 & 1 & 13 & -28 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

e, portanto, M tem apenas um fator invariante que é 1. As equações de M são:

$$\begin{aligned} x_3 &\equiv 0 \,(\mathrm{mod}\, 1) \\ x_4 &\equiv 0 \,(\mathrm{mod}\, 1) \\ 2x_1 + x_2 - 4x_3 + 13x_4 &\equiv 0 \,(\mathrm{mod}\, 1) \\ -5x_1 - 3x_2 + 9x_3 - 28x_4 &= 0. \end{aligned}$$

Como as três primeiras equações são triviais, concluimos que:

$$(x_1, x_2, x_3, x_4) \in M \text{ se e só se } -5x_1 - 3x_2 + 9x_3 - 28x_4 = 0.$$

O teorema seguinte é o último ingrediente para a demonstração do teorema de estrutura para grupos comutativos finitamente gerados.

Teorema 2.2.1. *Seja M um subgrupo de $\mathbb{Z}^n$ com fatores invariantes $d_1, \ldots, d_r$. Então, o grupo $\mathbb{Z}^n/M$ é isomorfo ao grupo $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$.*

Demonstração. *Seja M um subgrupo de $\mathbb{Z}^n$ com fatores invariantes $d_1, \ldots, d_r$. Pela Proposição 2.2.8, existe uma base de $\mathbb{Z}^n$, $\{f_1, \ldots, f_r, \ldots, f_n\}$ e uma base de M da forma $\{d_1 f_1, \ldots, d_r f_r\}$.*

Consideremos a correspondência ϕ que a cada elemento

$$(z_1 f_1 + z_2 f_2 + \ldots + z_r f_r + \ldots + z_n f_n) + M \;\; de \;\; \mathbb{Z}^n/M, \;\; (z_i \in \mathbb{Z} \;\; para\ todo \;\; 1 \leq i \leq n)$$

faz corresponder o elemento

$$\left([z_1]_{d_1}, [z_2]_{d_2}, \ldots, [z_r]_{d_r}, z_{r+1}, \ldots, z_{r+(n-r)}\right) \;\; de \;\; \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}.$$

É simples ver que esta correspondência é uma aplicação de $\mathbb{Z}^n/M$ *em* $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$.

Cálculos de rotina mostram que ϕ *é um morfismo:*

$$\begin{aligned}\phi\left[\left(\left(\sum_{i=1}^{n} z_i f_i\right)+M\right)+\left(\left(\sum_{i=1}^{n} t_i f_i\right)+M\right)\right] &= \phi\left[\left(\sum_{i=1}^{n}(z_i+t_i)\, f_i\right)+M\right] \\ &= \left([z_1+t_1]_{d_1}, \ldots [z_r+t_r]_{d_r}, (z_{r+1}+t_{r+1}), \ldots, (z_n+t_n)\right) \\ &= \left([z_1]_{d_1}, \ldots, [z_r]_{d_r}, z_{r+1}, \ldots, z_n\right) + \left([t_1]_{d_1}, \ldots, [t_r]_{d_r}, t_{r+1}, \ldots, t_n\right) \\ &= \phi\left(\left(\sum_{i=1}^{n} z_i f_i\right)+M\right) + \phi\left(\left(\sum_{i=1}^{n} t_i f_i\right)+M\right).\end{aligned}$$

A aplicação ϕ *é também injetiva, já que, se* $[z_i]_{d_i} = [t_i]_{d_i}$ *para qualquer* $1 \le i \le r$, *então* $z_i - t_i \in d_i\mathbb{Z}$, *para todo o* $i \in \{1, \ldots, r\}$ *e, portanto,*

$$(z_1 - t_1)\, f_1 + (z_2 - t_2)\, f_2 + \ldots + (z_r - t_r)\, f_r \in M,$$

o que significa que $(z_1 f_1 + \ldots + z_r f_r) + M = (t_1 f_1 + \ldots + t_r f_r) + M$. *Deste modo,*

$$\left([z_1]_{d_1}, \ldots, [z_r]_{d_r}, z_{r+1}, \ldots, z_n\right) = \left([t_1]_{d_1}, \ldots, [t_r]_{d_r}, t_{r+1}, \ldots, t_n\right) \Rightarrow \left(\sum_{i=1}^{n} z_i f_i\right) + M = \left(\sum_{i=1}^{n} t_i f_i\right) + M$$

isto é,

$$\phi\left(\left(\sum_{i=1}^{n} z_i f_i\right)+M\right) = \phi\left(\left(\sum_{i=1}^{n} t_i f_i\right)+M\right) \Rightarrow \left(\sum_{i=1}^{n} z_i f_i\right) + M = \left(\sum_{i=1}^{n} t_i f_i\right) + M.$$

A sobrejetividade de ϕ *é óbvia. Logo* ϕ *é um isomorfismo de* $\mathbb{Z}^n/M$ *em* $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$.

■

Da proposição 1.4.7, sabemos que qualquer grupo comutativo finitamente gerado é isomorfo a um grupo quociente $\mathbb{Z}^n/M$ para algum subgrupo M de $\mathbb{Z}^n$. Então, tendo em atenção o Teorema 2.2.1, concluimos que qualquer grupo comutativo finitamente gerado é isomorfo a um produto direto $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$, onde $d_1, \ldots, d_r$ são fatores invariantes de M.

Temos assim, o seguinte teorema de estrutura para grupos abelianos finitamente gerados:

Teorema 2.2.2. *Seja G um grupo comutativo finitamente gerado. Então existem números naturais* $\{d_i\}$, $i \in \{1,...,n\}$ *e k tais que:*

i) d_i *divide* d_{i+1}, *para qualquer* $1 \leq i \leq n-1$;

ii) G é isomorfo a $\mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$.

■

Capítulo 3

Monóides cancelativos finitos

Neste capítulo estudamos a classe dos monóides cancelativos que são finitos: mostramos que esta classe coincide com a classe dos grupos finitos e vemos como é que isso se reflete nas equações do subgrupo de $\mathbb{Z}^n$ associado ao monóide inicial.

Monóides cancelativos finitos são, naturalmente, finitamente gerados. Assim, começamos por considerar um monóide S comutativo, cancelativo e finitamente gerado e, com o teorema de estrutura para grupos abelianos finitamente gerados presente, identificamos o submonóide de $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$ isomorfo a S.

Se $S = \langle s_1, \ldots, s_n \rangle$ é um monóide finitamente gerado, a aplicação $f : \mathbb{N}^n \to S$ definida por

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i s_i$$

é um epimorfismo (Proposição 1.4.1). Deste modo, $S = f(\mathbb{N}^n) \cong \mathbb{N}^n / Nuc\, f$. Uma vez que $Nuc\, f$ é uma congruência, o conjunto $M = \{a - b : a, b \in \mathbb{N}^n, (a,\ b) \in Nuc\, f\}$ é um subgrupo de $\mathbb{Z}^n$. Se o monóide S for também cancelativo, então $\mathbb{N}^n / Nuc\, f$ é cancelativo e, pela Proposição 1.4.5, $Nuc\, f = \sim_M$, onde $\sim_M = \{(a,b) \in \mathbb{N}^n \times \mathbb{N}^n : a - b \in M\}$. Assim, se S é um monóide cancelativo finitamente gerado, $S \cong \mathbb{N}^n / Nuc\, f$. Pela Proposição 1.4.6, $\mathbb{N}^n / Nuc\, f$ é isomorfo ao submonóide $\left\{[a]_{\equiv_M} : a \in \mathbb{N}^n\right\}$ do grupo $\mathbb{Z}^n / \equiv_M$. Se $d_1, d_2 \ldots, d_r$ representarem os fatores invariantes de M, o Teorema 2.2.1 garante que $\mathbb{Z}^n / \equiv_M$ é isomorfo a $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$. Portanto, S é isomorfo a um submonóide do grupo $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$.

A proposição que se segue identifica o submonóide de $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$ isomorfo a S.

Proposição 3.1. Seja M um subgrupo de $\mathbb{Z}^n$, com fatores invariantes $d_1, d_2 ..., d_r$ e tal que $(x_1, x_2, ..., x_n) \in M$ se e só se

$$\begin{aligned} &a_{11}x_1 + ... + a_{1n}x_n \equiv 0 \,(\bmod d_1) \\ &a_{21}x_1 + ... + a_{2n}x_n \equiv 0 \,(\bmod d_2) \\ &... \\ &a_{r1}x_1 + ... + a_{rn}x_n \equiv 0 \,(\bmod d_r) \end{aligned}$$

$$\begin{aligned} &a_{(r+1)1}x_1 + ... + a_{(r+1)n}x_n = 0 \\ &... \\ &a_{n1}x_1 + ... + a_{nn}x_n = 0 \end{aligned}$$

Então $\mathbb{N}^n / \sim_M$ é isomorfo ao submonóide S de $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} ... \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$ gerado por

$$\left\{ \left([a_{11}]_{d_1}, ..., [a_{r1}]_{d_r}, a_{(r+1)1}, ..., a_{n1} \right), ..., \left([a_{1n}]_{d_1}, ..., [a_{rn}]_{d_r}, a_{(r+1)n}, ..., a_{nn} \right) \right\}$$

onde $[a]_d$ representa a classe de equivalência de a em $\mathbb{Z}_d$.

Demonstração. *Comecemos por observar que, uma vez que M é um subgrupo de* $\mathbb{Z}^n$*, a relação* $\sim_M = \{(a,b) \in \mathbb{N}^n \times \mathbb{N}^n : a - b \in M\}$ *é uma congruência em* $\mathbb{N}^n \times \mathbb{N}^n$.

Consideremos a correspondência ϕ *assim definida: para qualquer* $[(a_1, a_2, ..., a_n)]_{\sim_M} \in \mathbb{N}^n / \sim_M$,

$$\phi\,[(a_1, a_2, ..., a_n)]_{\sim_M} = \left(\left[\sum_{i=1}^{n} a_i a_{1i} \right]_{d_1}, ..., \left[\sum_{i=1}^{n} a_i a_{ri} \right]_{d_r}, \sum_{i=1}^{n} a_i a_{(r+1)i}, ..., \sum_{i=1}^{n} a_i a_{ni} \right).$$

A correspondência ϕ *é uma aplicação. De facto, para quaisquer* $(a_1, ..., a_n), (b_1, ..., b_n) \in \mathbb{N}^n$, *temos:*

$$[(a_1, a_2, ..., a_n)]_{\sim_M} = [(b_1, b_2, ..., b_n)]_{\sim_M} \Rightarrow (a_1 - b_1, ..., a_n - b_n) \in M \Rightarrow$$

$$\Rightarrow \begin{cases} a_{11}(a_1 - b_1) + ... + a_{1n}(a_n - b_n) \equiv 0 \,(\bmod d_1) \\ ... \\ a_{r1}(a_1 - b_1) + ... + a_{rn}(a_n - b_n) \equiv 0 \,(\bmod d_r) \\ a_{(r+1)1}(a_1 - b_1) + ... + a_{(r+1)n}(a_n - b_n) = 0 \\ ... \\ a_{n1}(a_1 - b_1) + ... + a_{nn}(a_n - b_n) = 0 \end{cases}$$

$$\Rightarrow \begin{cases} a_{11}a_1 + \ldots + a_{1n}a_n \equiv a_{11}b_1 + \ldots + a_{1n}b_n \,(\mathrm{mod}\, d_1) \\ \ldots \\ a_{r1}a_1 + \ldots + a_{rn}a_n \equiv a_{r1}b_1 + \ldots + a_{rn}b_n \,(\mathrm{mod}\, d_r) \\ a_{(r+1)1}a_1 + \ldots + a_{(r+1)n}a_n = a_{(r+1)1}b_1 + \ldots + a_{r+1}b_n \\ \ldots \\ a_{n1}a_1 + \ldots + a_{nn}a_n = a_{n1}b_1 + \ldots + a_{nn}b_n \end{cases}$$

$$\Rightarrow \begin{cases} \left[\sum_{i=1}^{n} a_{1i}a_i\right]_{d_1} = \left[\sum_{i=1}^{n} a_{1i}b_i\right]_{d_1} \\ \ldots \\ \left[\sum_{i=1}^{n} a_{ri}a_i\right]_{d_r} = \left[\sum_{a_{ri}b_i}\right]_{d_r} \\ \sum_{i=1}^{n} a_{(r+1)i}a_i = \sum_{i=1}^{n} a_{(r+1)i}b_i \\ \ldots \\ \sum_{i=1}^{n} a_{ni}a_i = \sum_{i=1}^{n} a_{ni}b_i \end{cases}$$

$$\Rightarrow \phi\left([(a_1,\ldots,a_n)]_{\sim_M}\right) = \phi\left([(b_1,\ldots,b_n)]_{\sim_M}\right)$$

Cálculos simples mostram que ϕ é um monomorfismo de monóides.

Finalmente, uma vez que ,

$$\phi\,[(a_1,a_2,\ldots,a_n)]_{\sim_M} = \left(\left[\sum_{i=1}^{n} a_i a_{1i}\right]_{d_1}, \ldots, \left[\sum_{i=1}^{n} a_i a_{ri}\right]_{d_r}, \sum_{i=1}^{n} a_i a_{(r+1)i}, \ldots, \sum_{i=1}^{n} a_i a_{ni}\right) =$$

$$= a_1\left([a_{11}]_{d_1}, [a_{21}]_{d_2} \ldots, [a_{r1}]_{d_r}, a_{(r+1)1}, \ldots, a_{n1}\right) + a_2\left([a_{12}]_{d_1}, [a_{22}]_{d_2} \ldots, [a_{r2}]_{d_r}, a_{(r+1)2}, \ldots, a_{n2}\right) + \ldots$$

$$\ldots + a_n\left([a_{1n}]_{d_1}, [a_{2n}]_{d_2}, \ldots, [a_{rn}]_{d_n}, a_{(r+1)n}, \ldots, a_{nn}\right)$$

segue-se que Imϕ é o submonóide de $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \ldots \times Z_{d_r} \times \mathbb{Z}^{n-r}$ gerado por

$$\left\{\left([a_{11}]_{d_1}, \ldots, [a_{r1}]_{d_r}, a_{(r+1)1}, \ldots, a_{n1}\right), \ldots, \left([a_{1n}]_{d_1}, \ldots, [a_{rn}]_{d_r}, a_{(r+1)n}, \ldots, a_{nn}\right)\right\}$$

■

Exemplo 3.1

Seja $M = \langle(-3,1,4),(1,5,-2)\rangle$ um subgrupo de $\mathbb{Z}^3$. Utilizando os resultados do Exemplo 2.2.1, temos:

$$\begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix} \cdot \begin{bmatrix} -3 & 1 & 4 \\ 1 & 5 & -2 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & 11 \\ 0 & 0 & 1 \\ 0 & 1 & 8 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$$ e, portanto, os fatores invariantes de

M são 1 e 2 e as equações de *M* são:

$$x_1 \equiv 0 \pmod 1$$
$$-2x_1 + x_3 \equiv 0 \pmod 2$$
$$11x_1 + x_2 + 8x_3 = 0.$$

Como a primeira equação é trivial, temos:
$(x_1, x_2, x_3) \in M$ se e só se $-2x_1 + x_3 \equiv 0 \pmod 2$ e $11x_1 + x_2 + 8x_3 = 0$.

Então , $\mathbb{N}^3/\sim_M$ é isomorfo ao submonóide de $\mathbb{Z}_1 \times \mathbb{Z}_2 \times \mathbb{Z}$ gerado por

$$\{([1]_1, [-2]_2, 11), ([0]_1, [0]_2, 1), ([0]_1, [1]_2, 8)\}.$$

que é isomorfo ao submonóide de $\mathbb{Z}_2 \times \mathbb{Z}$ gerado por

$$\{([-2]_2, 11), ([0]_2, 1), ([1]_2, 8)\}.$$

A próxima proposição carateriza os monóides finitos que são cancelativos.

Proposição 3.2. Seja *S* um monóide finito. Então *S* é cancelativo se e só se *S* é grupo.

Demonstração. *Seja S um monóide finito. É claro que se S é um grupo, S é cancelativo. Reciprocamente, suponhamos que S é cancelativo. Se* $S = \{0_S\}$*, S é grupo. Suponhamos que* $S \neq \{0_S\}$ *e seja* $s \in S \setminus \{0_S\}$*. Como S é finito, o subconjunto* $\{ns : n \in \mathbb{N}\}$ *de S é também finito pelo que* $ms = ns$ *para certos* $m, n \in \mathbb{N}$ *tais que* $m < n$*. De* $m < n$ *obtemos* $n - m > 0$*; temos, de facto, que* $n - m > 1$ *uma vez que, se* $n = m + 1$*, dado que S é cancelativo, teríamos*

$$ms = ns \Rightarrow ms + 0_S = ms + s \Rightarrow s = 0_S,$$

o que não acontece. Portanto $n - m > 1$ *e, logo* $n - m - 1 > 0$*. Assim,* $(n-m-1)s + s = (n-m-1+1)s = (n-m)s = 0_S$*, o que significa que* $(n-m-1)s$ *é o simétrico de s. Dada a arbitrariedade de s em* $S \setminus \{0_S\}$*, concluimos que S é grupo.*

■

Sabemos que qualquer monóide cancelativo finitamente gerado S é isomorfo a um monóide quociente $\mathbb{N}^n/\sim_M$ para certo natural n e certo subgrupo M de $\mathbb{Z}^n$. Acontece que, se S é finito, isto é, se $\mathbb{N}^n/\sim_M$ é finito, as equações de M assumem uma forma especial. A próxima proposição indica essa forma.

Proposição 3.3. Seja M um subgrupo de $\mathbb{Z}^n$. As seguintes afirmações são equivalentes:

i) $\mathbb{N}^n/\sim_M$ é finito;

ii) $\dim(M) = n$;

iii) Nenhuma equação de M é da forma $a_1x_1 + \ldots + a_nx_n = 0$.

Demonstração. *Provamos a seguinte sequência de implicações:*

$$i) \Rightarrow ii) \Rightarrow iii) \Rightarrow i)$$

$i) \Rightarrow ii)$

Sabemos que $\dim\mathbb{Z}^n = n$. *Seja* $(e_1, e_2, \ldots, e_n)$ *a base canónica de* $\mathbb{Z}^n$. *Como* $\mathbb{N}^n/\sim_M$ *é finito, para cada i, o subconjunto* $\{k[e_i]_{\sim_M} : k \in \mathbb{N}\setminus\{0\}\}$ *de* $\mathbb{N}^n/\sim_M$ *é finito. Com um argumento semelhante ao apresentado na Proposição* 3.2., *obtemos* $k_1, \ldots, k_n \in \mathbb{N}\setminus\{0\}$ *tais que* $k_i[e_i]_{\sim_M} = 0$, *para todo o i, isto é, tendo em conta a definição de* $\sim_M$, $k_ie_i \in M$. *Tem-se, assim, n elementos* $k_1e_1, k_2e_2, \ldots, k_ne_n$ *linearmente independentes de M. Como M é um subgrupo de* $\mathbb{Z}^n$ *e* $\dim\mathbb{Z}^n = n$, *segue-se que* $\dim(M) = n$.

$ii) \Rightarrow iii)$

Como $\dim(M) = n$, *o subespaço vetorial* $V = \langle M\rangle$ *de* $\mathbb{Q}^n$ *coincide com* $\mathbb{Q}^n$. *Se M admitisse uma equação homogénea, digamos,* $a_1x_1 + \ldots + a_nx_n = 0$, *então teríamos que* $(a_1, \ldots, a_n) \in V^\perp = (\mathbb{Q}^n)^\perp = \{0_{\mathbb{Q}^n}\}$ *(* $(x_1, x_2, \ldots, x_n)$ *é um vetor arbitrário de V) e, portanto,* $a_i = 0$ *para todo o i, o que não pode suceder porque, a existirem,* $a_1, a_2, \ldots, a_n$ *são as entradas de uma coluna de uma matriz invertível.*

iii) $\Rightarrow$ *i*)

Tendo em conta a hipótese, as equações de M são do tipo:

$$\begin{aligned} &a_{11}x_1 + \ldots + a_{1n}x_n \equiv 0 \,(\bmod d_1) \\ &a_{21}x_1 + \ldots + a_{2n}x_n \equiv 0 \,(\bmod d_2) \\ &\ldots \\ &a_{r1}x_1 + \ldots + a_{rn}x_n \equiv 0 \,(\bmod d_r) \end{aligned}$$

onde d_i *divide* d_{i+1} *para todo o i. Então, para cada i,* d_i *divide* d_r *e, como* $d_r e_i = (0, \ldots, d_r, \ldots, 0)$, *obtemos:*

$$\begin{aligned} &a_{1i}d_r \equiv 0 \,(\bmod d_1) \\ &a_{2i}d_r \equiv 0 \,(\bmod d_2) \\ &\ldots \\ &a_{ri}d_r \equiv 0 \,(\bmod d_r) \end{aligned}$$

pelo que $d_r e_i \in M$, *para cada i.*

Assim, $d_r [e_i]_{\sim_M} = [0]_{\sim_M}$ *no monóide* $\mathbb{N}^n / \sim_M$. *Como cada elemento de* $\mathbb{N}^n / \sim_M$ *é da forma* $\sum_{i=1}^{n} a_i [e_i]_{\sim_M}$, *com* $a_i \in \{0, d_1, \ldots, d_r - 1\}$, *segue-se que* $\mathbb{N}^n / \sim_M$ *tem, no máximo,* $(d_r)^n$ *elementos. Portanto, o monóide* $\mathbb{N}^n / \sim_M$ *é finito.*

■

Corolário 3.1. Seja M um subgrupo de $\mathbb{Z}^n$ de dimensão n e com fatores invariantes $d_1, \ldots, d_n$.

Então:

i) $\mathbb{N}^n / \sim_M$ é um grupo finito;

ii) M contém um elemento fortemente positivo;

iii) $\mathbb{N}^n / \sim_M$ é isomorfo a $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_n}$.

Demonstração. *i) Como o monóide* $\mathbb{N}^n / \sim_M$ *é cancelativo, se ele é finito, obtemos pela Proposição* 3.2. *que* $\mathbb{N}^n / \sim_M$ *é um grupo. Ora, por hipótese, M tem n fatores invarian-*

tes, logo $\dim(M) = n$ *(uma vez que* $(d_1e_1,\ldots,d_ne_n)$ *é uma base de M) e, pela Proposição* 3.3. *isso equivale a dizer que* $\mathbb{N}^n/\sim_M$ *é finito.*

ii) Consequência imediata de 2 da Proposição 1.4.7.

iii) Pela Proposição 3.1., $\mathbb{N}^n/\sim_M$ *é isomorfo ao submonóide de* $\mathbb{Z}_{d_1}\times\ldots\times\mathbb{Z}_{d_n}$ *gerado por* $\left\{\left([a_{11}]_{d_1},\ldots,[a_{n1}]_{d_n}\right),\left([a_{12}]_{d_1},\ldots,[a_{n2}]_{d_n}\right),\ldots,\left([a_{1n}]_{d_1},\ldots,[a_{nn}]_{d_n}\right)\right\}$*, isto é,* $\mathbb{N}^n/\sim_M$ *é isomorfo a* $\mathbb{Z}_{d_1}\times\ldots\times\mathbb{Z}_{d_n}$.

■

Exemplo 3.2.

Seja $M = \langle(3,2,-1),(4,-1,5),(2,-1,7)\rangle$ um subgrupo de $\mathbb{Z}^3$, de dimensão 3. Os fatores invariantes de M são $d_1 = d_2 = 1$ e $d_3 = 28$ (Exemplo 2.2.3).

Então, $\mathbb{N}^3/\sim_M$ é isomorfo a $\mathbb{Z}_1\times\mathbb{Z}_1\times\mathbb{Z}_{28}$ e é, por isso, finito.

Exemplo 3.3.

Determinando os fatores invariantes do subgrupo $M = \langle(2,-4,2),(-6,2,2),(-2,2,4)\rangle$ de $\mathbb{Z}^3$, de dimensão 3, obtemos $d_1 = d_2 = 2$ e $d_3 = 22$.

Então, $\mathbb{N}^3/\sim_M$ é isomorfo a $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_{22}$.

Bibliografia

Finitely generated monoids, J.C. Rosales and P.A. García-Sanchéz. Nova Science Pub Inc (June 1999)